Department of Justice

Office of the Chief Information Officer

IT Governance Guide

May 2008

Version 5.0

Document Approval Form

Title of Document: **IT Governance Guide**

Version: 5.0 Date: May 2008

If a check is next to your title, please sign and date to approve.

☒ Chief Information Officer, DOJ, *Vance Hitch*

Sign: Vance Hitch Date: 5/28/08

☒ Deputy CIO, Enterprise Solutions, *John Murray*

Sign: John Murray Date: 5/16/08

☒ Deputy CIO, Policy and Planning, *Kent Holtgrewe*

Sign: FOR KENT HOLTGREWE Date: 5/22/08

☒ Deputy CIO, IT Security, *Kevin Deeley* (Acting)

Sign: Date: 5/16/08

Office of the Chief Information Officer

Department of Justice

Office of the Chief Information Officer

IT Governance Guide

Version 5.0

May 2008

Table of Contents

Table of Figures

Executive Summary

Chief Information Officers (CIOs) of Federal agencies are responsible for developing, implementing and maintaining a process to maximize the value and assess and manage the risks of agency IT investments. The Department of Justice's (DOJ) Office of the Chief Information Officer (OCIO) established an IT governance program to define and integrate new and existing governance processes to accomplish these objectives. The Information Technology (IT) governance program is developing, establishing and improving the Department's IT management practices through incremental process development and iterative process integration and improvement.

Version 5.0 of the "IT Governance Guide" is the fifth edition of the Department's governance guidance. This version of the Guide refines and augments the previously documented IT governance processes and products and incorporates process improvements resulting from lessons learned or changes in policy.

Version 5.0 of the Guide incorporates the following major improvements:

- Explanation of the Department's *Definition of IT* – This guidance update is intended to reduce discrepancies in IT cost reporting. The definition provides a detailed description of the elements of IT costs and uses several examples to illustrate the various types of IT investments. The definition is located in Appendix B.

- Incorporates two additional elements into the Governance Framework.

  System Development Life Cycle (SDLC) Framework – Responding to an audit recommendation from the Office of the Inspector General, the Department established minimum SDLC documentation and review requirements for IT development projects and defined the compliance responsibilities for the Department, Component and IT project managers.

  Enterprise Performance Management Model – This new model describes the Department's approach for implementing a standard methodology for evaluating IT investment performance. This new element of the IT governance framework defines how program outcomes and IT investment performance will be linked.

- Augments the Oversight Review descriptions to incorporate new requirements and to clarify stakeholder responsibilities for compliance.

  Executive Review Process – Recent appropriations law requires the Department Investment Review Board (DIRB) to certify that designated high cost development projects have appropriate oversight mechanisms in place. This new requirement was incorporated into the current Executive Review Process. A major update to the Executive Review Process is planned for the next version of the Guide.

  Compliance Review Process – An improved description of the Department's IT Security Review Process clarifies the purpose of the various security compliance reviews and highlights the responsibilities of the Department, Component and IT project managers.

1. Introduction

1.1 Purpose

The primary purpose of this Guide is to communicate the expectations for the stakeholders involved in the execution and oversight of the Department's Information Technology (IT) governance. It is a companion document to the Department's IT policy order – Department of Justice (DOJ) Information Resources Management (IRM) DOJ Order 2880.1B. Responsibility for the governance of the Department's IT investments resides primarily with the Department's Chief Information Officer (CIO), working in concert with the Department's Chief Financial Officer (CFO). Key stakeholders include the Office of the Chief Information Officer (OCIO), the Department's Budget Staff, the Component CIOs, the Component business leaders who invest in IT and the Component budget / finance offices. A more extensive list of stakeholders can be found in Section 2.3.

The Guide also communicates the Department's self-governance expectations to Components that directly manage IT services or investments. The list of Department Components in Appendix A identifies the Components that do not directly manage IT services or investments and are not expected to implement the self-governance actions described in this document.

Finally, the Guide communicates the Department's IT governance practices to external oversight organizations such as the Office of Management and Budget (OMB), the Government Accountability Office (GAO) and the Department's Office of the Inspector General (OIG).

1.2 Definition of IT

According to the Clinger-Cohen Act of 1996 Information Technology is defined as "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the [Department]. 'Information technology' includes computers, ancillary equipment, software, software maintenance and support, firmware and similar procedures, services (including support services) and related resources."

In order to understand and apply the IT definition above, the OCIO has provided guidance to help clarify what the Department considers to be Information Technology. This guidance will help to ensure full and consistent reporting of IT costs across the Department. Information Technology at the DOJ supports wide and diverse missions and goals and is composed of three broad categories: Mission-Delivery and Business Solutions; IT Infrastructure; and IT Practices and Management. The Department's guidance on the definition of IT and associated examples can be found in Appendix B.

1.3 Background

Beginning more than ten years ago, Federal legislative mandates have steadily increased the oversight and reporting requirements for acquisition and management of IT resources. These mandates identify the Department CIO as the person responsible for monitoring and managing the performance of Department IT investments and for advising the Attorney General when ongoing investments should be modified, replaced or terminated. To comply with these mandates, the Department's OCIO has developed and implemented an integrated IT governance process that seeks to maximize the value and assess and manage the risks associated with acquisition and management of IT investments. The Department's governance efforts concentrate on improving the process for investment selection and ensuring appropriate investment oversight is performed throughout the investment's life cycle.

The CIO's IT governance responsibilities are administered by four of the five OCIO staffs. The Policy and Planning Staff is responsible for facilitating and coordinating the planning efforts that drive IT investment selection and funding through the Federal budget process. The Enterprise Solutions, E-Government Services and IT Security Staffs are responsible for communicating IT related guidance, performing Department-level oversight reviews, reporting on the overall health and compliance of selected investments and supporting the investment planning and selection processes. The fifth OCIO staff, the Operations Services Staff, does not have Department-level IT governance responsibilities, but is responsible for providing a wide range of IT services including common desktop, telecommunications and IT infrastructure services.

1.4 Drivers

There are three main drivers for the Department's IT governance program: legislative requirements and oversight, DOJ mission needs and audit findings and recommendations.

Legislative Requirements and Oversight. Four oversight bodies monitor the Department's implementation of legislative and regulatory requirements and provide guidance based on best practices. These agencies are: the Office of Management and Budget (OMB), the Government Accountability Office (GAO), the DOJ Office of the Inspector General (OIG) and Congress. Appendix C contains a table that lists the most significant legislative and regulatory requirements for IT governance and identifies how each requirement is addressed in this Guide.

DOJ Mission Needs. Internal drivers primarily come from two sources: the Attorney General's (AG) Office in the form of strategic mission and business priorities communicated in the Department's Strategic Plan and the Department CIO in the form of strategic IT goals and priorities communicated in the Department's IT Strategic Plan. These goals and priorities serve as criteria for investment selection and budget decisions in the planning and budget phases of the IT investment life cycle.

Audit Findings and Recommendations. Audits of the Department's IT programs and investments by GAO and OIG sometimes identify weaknesses in management practices and policies that must be corrected. Improvements to IT policies, practices and management processes implemented to address recommendations from an audit must be officially documented and implemented. This Guide is one of the documents used to officially implement Department policies for IT governance processes and procedures.

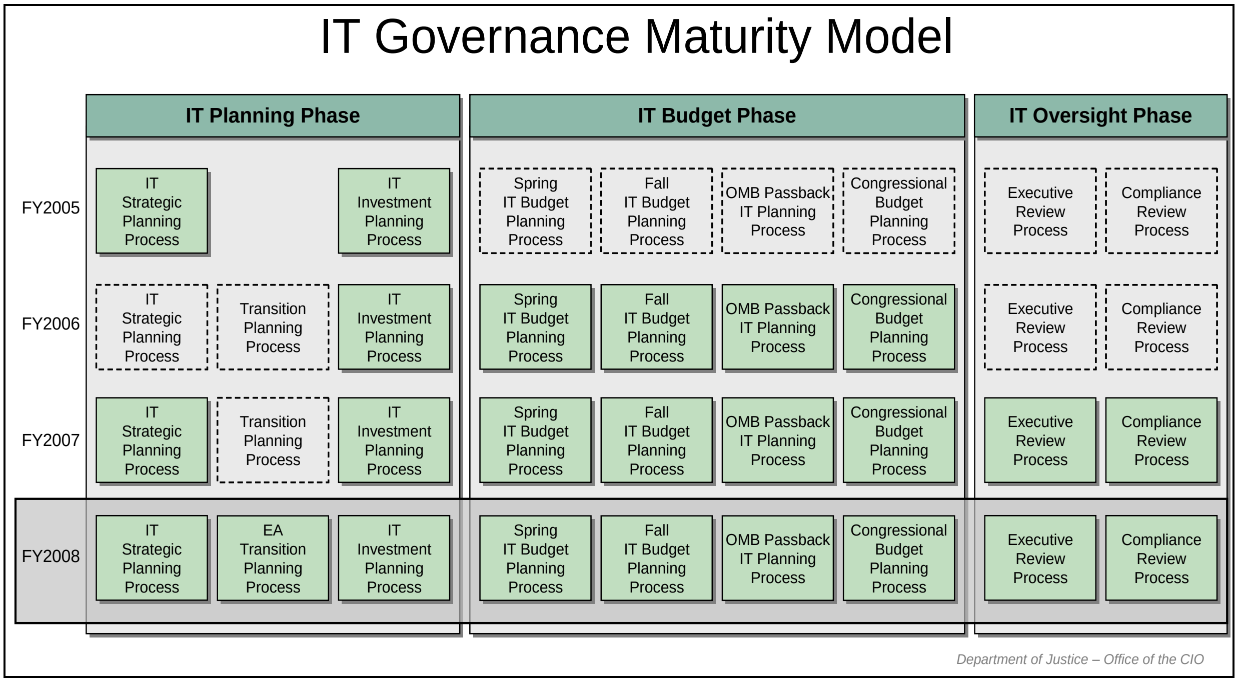
1.5 Goals

The goals of the Department's IT governance program are:

- Satisfy statutory and regulatory IT management requirements.
- Inform and impact Department and Component IT investment decisions to ensure that constrained IT resources are efficiently used to further the Department's goals and continue to deliver the expected performance results.

1.6 Governance Maturity and Evolution

The Department's IT governance processes have evolved over the past several years and continue to mature as the Department works to continuously improve and integrate IT management processes into a more cohesive set of actions. The Department OCIO began by establishing a governance framework consisting of three life cycle phases - IT Planning Phase, IT Budget Phase and IT Oversight Phase - supported by a series of integrated planning and oversight processes. Then the Department employed a phased approach that focused first on developing and implementing IT planning processes, then targeted IT budget planning and budget development and finally integrated the various oversight processes into the framework.



IT Governance Maturity Model

	IT Planning Phase			IT Budget Phase				IT Oversight Phase	
FY2005	IT Strategic Planning Process		IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Planning Process	Congressional Budget Planning Process	Executive Review Process	Compliance Review Process
FY2006	IT Strategic Planning Process	Transition Planning Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Planning Process	Congressional Budget Planning Process	Executive Review Process	Compliance Review Process
FY2007	IT Strategic Planning Process	Transition Planning Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Planning Process	Congressional Budget Planning Process	Executive Review Process	Compliance Review Process
FY2008	IT Strategic Planning Process	EA Transition Planning Process	IT Investment Planning Process	Spring IT Budget Planning Process	Fall IT Budget Planning Process	OMB Passback IT Planning Process	Congressional Budget Planning Process	Executive Review Process	Compliance Review Process

Department of Justice – Office of the CIO

Figure 1-1. IT Governance Maturity Model

The IT Governance Maturity Model shown in Figure 1-1 illustrates the sequence in which the IT governance processes of the three life cycle phases were developed and implemented over the course of the past four Fiscal Years.[1] The processes in the figure above are being continuously improved by applying lessons learned and stakeholder feedback that are collected at the end of each planning cycle. This document, version 5.0, refines and augments the established IT governance processes and products to incorporate process improvements and to address new regulatory and statutory requirements.

1.7 New in Version 5.0.

Update to the Definition of IT.

- This expanded guidance is intended to clarify what the Department considers to be Information Technology and is therefore managed by the IT governance processes.

New Models. Two new models are integrated into the IT governance framework.

- SDLC Framework – Relates the Department's standard system development guidance to the investment life cycle, establishes minimum planning and evaluation activities and artifacts that must be prepared during the course of a system development project and describes the responsibilities of key stakeholders in applying the SDLC – Section 2.4.
- Enterprise Performance Management Model – Describes the Department's approach for standard measurement of investment performance – Section 2.5.

New in Version 5.0

Update to the Definition of IT

- Appendix B

Two new models:

- SDLC Framework
- Enterprise Performance Management (EPM) Model

Augmentation of Two Processes:

- Congressional Certification Review
- IT Security Review Process

Updates to Existing Models and Processes:

- Stakeholder Model
- Investment Classification Model
- EA Transition Planning Process
- OMB Passback IT Planning Process
- EA Review Process

Augmentation of two Oversight Processes.

- Executive Review Process – Incorporates the requirement for the Department to certify that selected IT programs meet the stipulations specified in Appropriations Law. – Section 3.3.1.

[1] The solid green boxes depict processes that were described or updated in the IT Governance Guide during each fiscal year. The boxes outlined with dotted lines represent processes that were described in a subsequent version of the guide.

- IT Security Review Process – Updates the description of the Departments IT security review process and clarifies the responsibilities of key stakeholders. – Section 3.3.2.5.

Updates to Existing Models and Processes.

- Stakeholder Model – Identifies new stakeholders who play significant roles in the Department's IT governance processes. – Section 2.3.
- Investment Classification Model – Updates the model to incorporate the definitions from the Department's guidance on the definitions of IT – Section 2.6
- EA Transition Planning Process – Incorporates process improvements from lessons learned – Section 3.1.2.
- OMB Passback IT Planning Process – Incorporates process improvement including guidance on redacting of OMB Exhibit 300s for public posting. – Section 3.2.3.
- EA Review Process – Incorporates process improvements from lessons learned. – Section 3.3.2.2.

Future Versions. Future updates to this Guide will be made to address areas of weakness discovered during process review, to incorporate lessons learned for continuous process improvement and to ensure that the governance program remains compliant with new and evolving legislative and regulatory requirements.

2. Governance Framework

2.1 Introduction to the Framework

IT governance is the act of planning and managing the Department's IT resources through a related set of managed processes. The IT governance framework provides the context and structure for binding together the cogs of the various governance processes so that they operate as a well-oiled machine. The governance framework consists of seven models that together provide the structure that links the moving parts of the governance processes.

- The **Investment Life Cycle Model** shows the sequence of governance processes from strategic inception, through reviewed operations, to final disposition. The model integrates the investment life cycle processes through the movement of standard products from one process to the next.
- The **Stakeholder Model** identifies the stakeholders (persons, groups, committees and organizations) who play significant roles in the Department's IT governance processes and shows how these stakeholders participate in the life cycle by relating them to processes and products.
- The **System Development Life Cycle (SDLC) Framework** provides a standard approach for completing key planning processes necessary for the orderly and effective development and implementation of information technology systems and identifies a minimum set of required artifacts to provide visibility and rigor into the development process.
- The **Enterprise Performance Management (EPM)** describes a standard approach for measuring investment performance in meeting mission / business needs across the IT portfolio.
- The **Investment Classification Model** provides a standard structure for categorizing investments for analysis and oversight.
- The **IT Oversight Model** provides a structure for integrating the Department's tiered oversight reviews into a unified governance structure.
- The **Component Self-Governance Model** identifies the self-governance actions Components must perform to manage their IT assets.

These seven models provide the structure for integrating the various aspects of IT governance throughout the Department. In this chapter we will use two example investments – Investment A that addresses a common business need for several Components and Investment B that meets a unique business need for a single Component – to illustrate how these models relate to one another as well as how each model applies to the management of individual IT investments.

2.2 Investment Life Cycle Model

The Investment Life Cycle Model is the backbone of the Department's IT governance framework and provides an end-to-end iterative sequence of processes for managing IT investments. The life cycle processes in the model are integrated through the logical and repeatable development and movement of IT management products from one process to the next while providing for periodic feedback to support the iterative cycle of planning, budgeting and oversight that recurs each fiscal year.

Different stakeholders are involved in directing, producing, reviewing and using the products developed by each process, so the success of the model relies on its ability to clearly define the products that are produced in one process and handed to another for further processing. Example Investments A and B, as well as all other investments in the Department's IT portfolio, are managed through these processes.

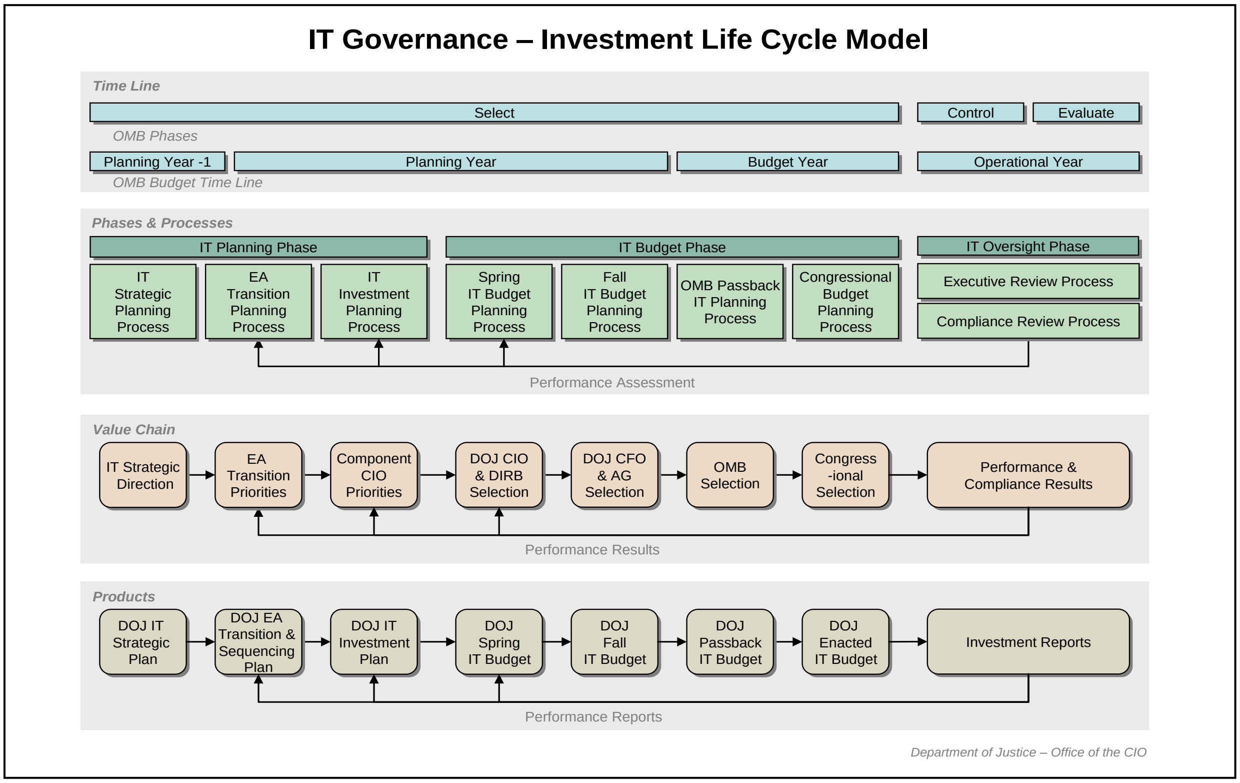


Figure 2-1. IT Governance - Investment Life Cycle Model

The Investment Life Cycle Model consists of four elements: the time line, the phases and processes, the value chain and the products.

Time Line. The time line is represented in blue at the top of the diagram. It aligns with the GAO ITIM and OMB budget planning timelines and is used to establish consistent timing for the processes in the Investment Life Cycle. The GAO Select-Control-Evaluate time line concept is used in conjunction with the OMB budget planning time line, which speaks in terms of the planning year, budget year and operation year. The three-year budget planning cycle serves as the generic time scale for scheduling the work of the three governance phases.

Phases & Processes. Three phases are used to encompass the governance work activities. These are shown in dark green. The processes within each phase are shown in lighter green. The phases are briefly described below. The governance processes are described individually in Section 3.

- In the **IT Planning Phase**, the Department CIO defines the Department's strategic IT direction, the transition strategies for moving forward and the investment priorities for the future.
- In the **IT Budget Phase** the Department CIO selects the Department's IT investments needed to achieve the Department's IT strategic goals and submits the investments for approval and funding through the Department and Federal budgeting processes.
- In the **IT Oversight Phase**, the Department monitors the development and on-going operations of the Department's investments to ensure that performance objectives are and continue to be met.

Value Chain. The third element of the Investment Life Cycle Model is the value chain, represented in orange. The value chain represents the business outcomes that result from each process.

> The **IT Strategic Direction** drives the EA tactical planning that results in an **EA Transition Direction.** The EA transition direction describes the approach for transforming the Department's IT enterprise to a desired future state and drives the **Component CIO Priorities** of IT investments needed to achieve the future state. The prioritized investments are routed through three key DOJ stakeholder groups for their input. First the **DOJ CIO** reviews the Component requests and presents a Department-level prioritization for Department Investment Review Board (**DIRB) Selection** at the annual DIRB portfolio review meeting. Second, the **DOJ CFO and AG Selection** takes place through the DOJ budget process. Third, the selected investments are then submitted with the Department budget for **OMB Selection,** which is followed by **Congressional Selection**. Investments approved by Congress are funded through the annual appropriations act. After the appropriated funds are received by the Department they are allotted for investment development, implementation, or operations, investment progress, performance and compliance. These investment actions are monitored through a variety of investment reports and review processes to ensure the planned **Performance and Compliance Results** are achieved.

Products. The fourth element of the Investment Life Cycle Model is the set of products that are the outputs of the processes. The products, shown in brown, contain the information produced by one process that is used by another process.

- **DOJ IT Strategic Plan.** The plan defines the Department's 3-5 year strategic goals and priorities for IT resources.
- **DOJ EA Transition and Sequencing Plan**. The plan describes the tactical approach for moving the Department's IT enterprise from its current architecture to the target architecture to support the IT strategic goals and priorities.

- **DOJ IT Investment Plan**. The plan prioritizes the IT investments needed to support strategic mission, business and IT goals.
- **DOJ Spring IT Budget**. The spring budget contains the priority IT investments for the DOJ Spring budget data call in concurrence with the Department Investment Review Board (DIRB).
- **DOJ Fall IT Budget**. The Fall budget is an update of the DOJ Spring IT Budget. It reflects the Attorney General’s decisions and is submitted to OMB in the early Fall.
- **DOJ Passback IT Budget.** In the late Fall, OMB returns the budget to the Department for update. The returned budget is called the OMB Passback. When the Department provides the updates and re-submits the budget to OMB – this is called the DOJ Passback IT Budget.
- **DOJ Enacted IT Budget.** This is the budget enacted by the Congress, which results in appropriated funding for IT investments.
- **Investment Reports**. These are the various reports prepared by project managers, Components and oversight groups that describe the progress, performance and compliance of the investments.

2.3 Stakeholder Model

The IT Governance Stakeholder Model identifies key stakeholders (persons, groups, committees, organizations), who play a role in the Department’s IT governance processes. These stakeholders participate at varying stages of the Department's IT governance Framework including the Investment Life Cycle. As with each investment in the Department's IT portfolio, Investments A and B will interact both directly and indirectly with many of these stakeholders throughout their life cycles.

There are five stakeholder groups:

- **Federal Oversight Groups** include external organizations who oversee the Department’s governance activities.
- **DOJ Oversight Groups** include the review boards, advisory Councils and committees who govern the Department’s IT investment activities.
- The **DOJ Office of the CIO (OCIO)** includes staff organizations under the Department CIO who are responsible for managing the Department’s IT investment management programs.
- **DOJ Partners** are the Department-level persons and organizations outside the DOJ OCIO who participate in or influence IT investment planning and management.
- **Component Partners** are the people and organizations within the Components responsible for performing or participating in IT investment management processes.

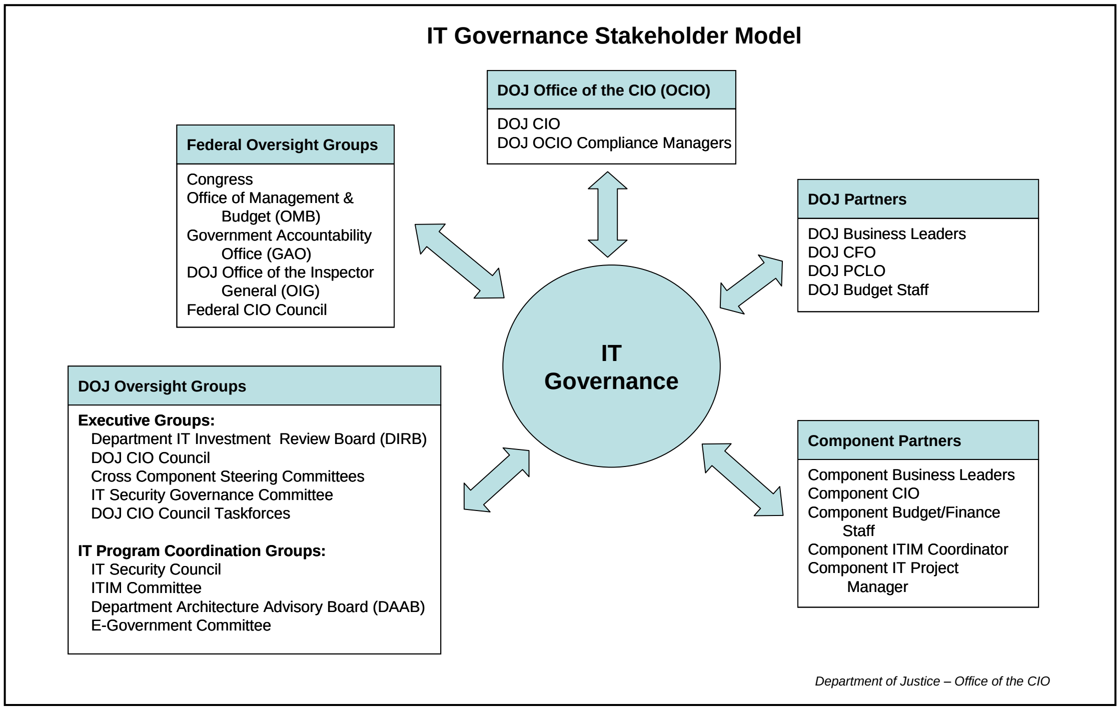

IT Governance Stakeholder Model
DOJ Office of the CIO (OCIO)
DOJ CIO
DOJ OCIO Compliance Managers
Federal Oversight Groups
Congress
Office of Management & Budget (OMB)
Government Accountability Office (GAO)
DOJ Office of the Inspector General (OIG)
Federal CIO Council
DOJ Partners
DOJ Business Leaders
DOJ CFO
DOJ PCLO
DOJ Budget Staff
IT Governance
DOJ Oversight Groups
Executive Groups:
Department IT Investment Review Board (DIRB)
DOJ CIO Council
Cross Component Steering Committees
IT Security Governance Committee
DOJ CIO Council Taskforces
IT Program Coordination Groups:
IT Security Council
ITIM Committee
Department Architecture Advisory Board (DAAB)
E-Government Committee
Component Partners
Component Business Leaders
Component CIO
Component Budget/Finance Staff
Component ITIM Coordinator
Component IT Project Manager
Department of Justice – Office of the CIO

Figure 2-2. IT Governance Stakeholder Model

The stakeholder groups shown in Figure 2-2 are described on the following pages.

Federal Oversight Groups:

- **Congress.** The legislative branch defines, authorizes and oversees the Department's operations through legislation and the appropriations process. The Congress may also periodically review the Department's IT program or the development and performance of selected high profile IT investments.
- **Office of Management and Budget (OMB).** As part of the Executive Office of the President, OMB performs oversight of Executive Branch IT investment management programs to ensure compliance with Federal laws and administration policy. OMB prepares the Federal budget for presentation to Congress and renders recommendations on funding levels for IT investments.
- **Government Accountability Office (GAO).** GAO audits executive agencies and programs for compliance with Federal laws, policies and best practices on behalf and at the request of the Congress. Both processes and IT investments are subject to GAO audit.
- **DOJ Office of the Inspector General (OIG).** The OIG is the Department's internal audit organization and is responsible for reviewing IT processes and investments to ensure compliance with best practices, Federal regulations and Department policies.
- **Federal CIO Council.** The Federal CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing and performance of Federal Government agency information resources. The Council's role

includes developing recommendations for information technology management policies, procedures and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's IT workforce.

DOJ Oversight Groups. There are two types of oversight groups within DOJ, Executive Governance Groups and IT Program Coordination Groups.

Executive Governance Groups. Governance bodies composed of senior executives with oversight and advisory responsibilities.

- **Department IT Investment Review Board (DIRB).** The Department IT Investment Review Board (DIRB) is an executive body that oversees the annual selection of the Department's IT investments for budget submission and conducts periodic reviews throughout the year of the Department's high profile, high cost, or high risk IT investments to ensure the expected return on investment (ROI) is delivered. The DIRB is chaired by the Deputy Attorney General (DAG) and the membership includes the Chief Information Officer (CIO) – who serves as Vice Chair, the Chief Financial Officer (CFO) and four other senior executives.
- **DOJ CIO Council.** The DOJ CIO Council is a Department-wide collaboration and advisory forum chartered and chaired by the DOJ CIO and composed of the CIOs from the Department's Components. The Council meets quarterly to review progress on strategic goals and to advise the DOJ CIO on IT management issues, including, strategic direction, policy and governance, investment priorities and enterprise architecture.
- **Executive Steering Committees.** These committees are comprised of executive stakeholders responsible for providing strategic direction and oversight of large common solution IT investments. Examples of Executive Steering Committees include the Litigation Case Management System (LCMS) Steering Committee, the Law Enforcement Information Sharing Program (LEISP) Steering Committee, the Joint Automated Booking System (JABS) Steering Committee and the Unified Financial Management System (UFMS) executive committee.
- **IT Security Governance Committee (ITSGC).** The ITSGC provides a forum and process for identifying high priority IT security-related topics, enhances communications with Component CIOs, obtains input from Subject Matter Experts (SMEs) and Mission stakeholders and provides informed advice to the DOJ CIO Council. Informed advice helps improve risk-based decisions for IT security governance and risk management as well as manage expectations and align strategies of IT stakeholders across the Department.

  The ITSGC is a sub-committee of the CIO Council that supports the DOJ CIO in making risk-based decisions on matters pertaining to enterprise IT security and risk management impacting the following key areas:
  - Strategy/Risk Management. Establishes the enterprise IT security risk management strategy and determines the strategic security objectives.
  - Investments/Projects. Aligns and prioritizes competing IT security investments and projects to implement the IT security risk management strategy.

  - IT Security Policy. Creates new or modifies existing policies in support of the enterprise IT security risk management strategy and enterprise security investment priorities.
  - IT Security Architecture. Modifies security architecture as needed to support enterprise IT security risk management strategy and enterprise security projects.

- **CIO Council Ad Hoc Task Forces.** The CIO Council Ad Hoc Task Forces are comprised of Component CIOs and other CIO Council members who collaborate to address common issues or develop strategies for leveraging solutions across multiple Components. Task Forces are formed when CIO Council members identify common issues of interest not being addressed by other senior level planning groups. Each Task Force is headed by one of the Component CIOs, who calls meetings of the group to define the group purpose, objectives and desired outcomes and to carry out the Task Force action plan. Task Forces will typically remain in place for a specified period, until the objectives of the group are completed, or until another mechanism is established to manage the issue that triggered formation of the Task Force. Ad Hoc Task Forces are currently formed to address the following issues: Identity Management, IT Records Management, IT Security and Common Services Prioritization. Task Forces report progress to the full CIO Council at the quarterly CIO Council meetings.

IT Program Coordination Groups. Committees composed of mid-level managers responsible for coordinating implementation of the Department's IT management policies and procedures.

- **IT Security Council.** The IT Security Council is a subcommittee of the DOJ CIO Council chartered by the DOJ CIO and chaired by the DOJ Chief IT Security Officer/Deputy CIO for IT Security. The Council serves as the forum for developing procedures and processes for implementing Federal and Department IT security policies, reviews IT security compliance issues and recommends solutions to the Chief IT Security Officer and affected CIOs.

- **ITIM Committee.** The IT Investment Management (ITIM) Committee is the subcommittee of the DOJ CIO Council that coordinates IT investment management activities and training and advises the DOJ CIO on ITIM policy, processes, procedures and reporting requirements. The committee is chaired by the DOJ OCIO Policy and Planning Staff Assistant Director.

- **Department Architecture Advisory Board (DAAB).** The Department Architecture Advisory Board (DAAB) provides oversight of the EA program at the Department level, tracks the progress of the EA program in meeting Department goals and advises the CIO Council on architecture policies and priorities. In addition, the DAAB sets EA policy for the Department, to include Framework and Methodology decision-making, determining the EA role in IT governance and ITIM, and the establishment and ongoing oversight of EA standards. The DAAB also assists in the development and communication of guidance and direction from the Department's Enterprise Architecture (EA) program to Component Agency EA programs, as well as receives feedback from the Components on various Department-wide EA policies and guidance. The DAAB is chaired by the DOJ Deputy CIO for Policy and Planning and the DOJ

Chief Enterprise Architect serves as the Vice-Chair. Participating members of the DAAB include Component Deputy CIOs and Component Enterprise Architects.

- **E-Government Committee.** The E-Government Committee (currently operating as the E-Gov Working Group) is the subcommittee of the CIO Council that communicates the Department's E-Government strategies and objectives. The group is composed of representatives from the Components and is chaired by the DOJ OCIO E-Government Services Staff Deputy Director. The group uses the President's Management Agenda (PMA) as a framework for addressing issues related to E-government services and solutions, including business model changes, organizational changes, policy and procedural changes, technical standards, protocols and technologies to support completion of the OMB approved DOJ E-Government Implementation Plan. The group chair advises the CIO on E-Gov-related policy and procedures and recommends solutions to issues raised by the E-Gov Committee members.

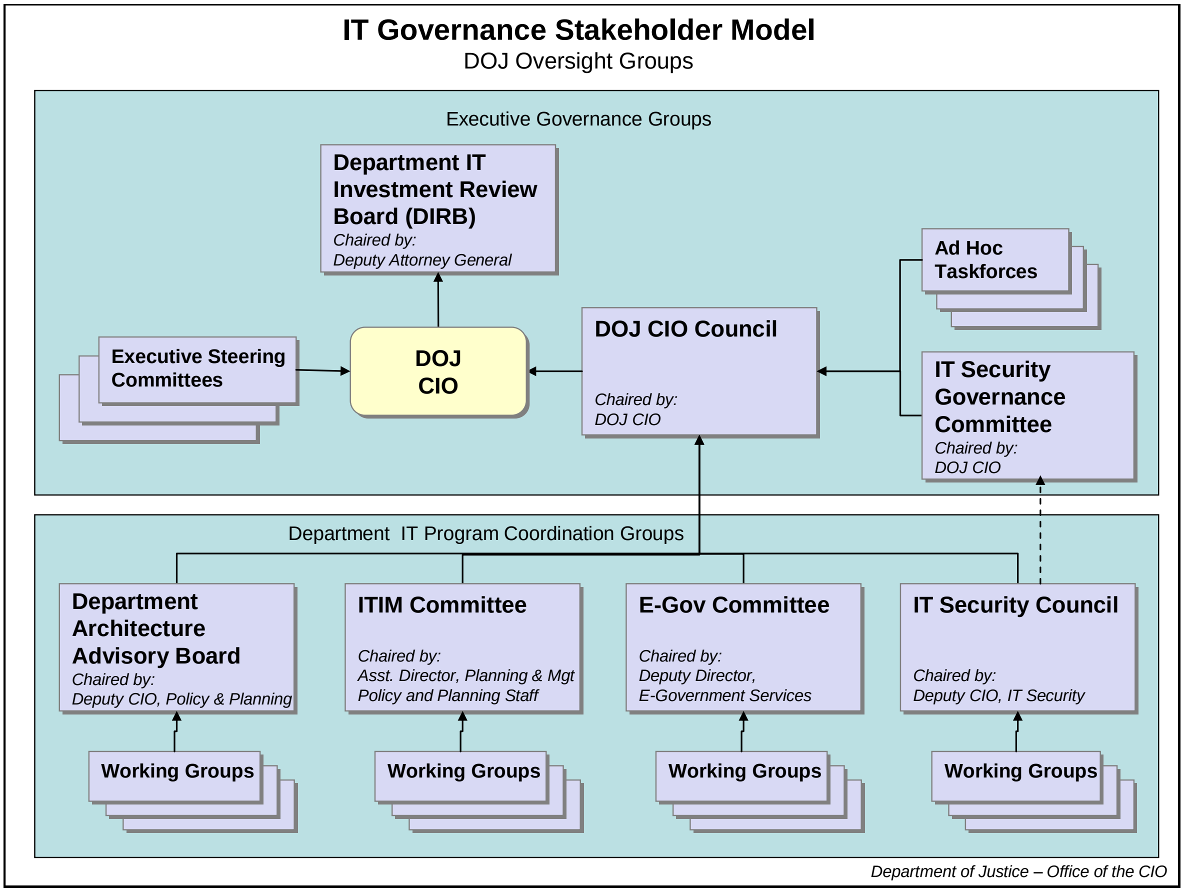

IT Governance Stakeholder Model
DOJ Oversight Groups
Executive Governance Groups
Department IT Investment Review Board (DIRB)
Chaired by:
Deputy Attorney General
Ad Hoc Taskforces
DOJ CIO Council
Chaired by:
DOJ CIO
Executive Steering Committees
DOJ CIO
IT Security Governance Committee
Chaired by:
DOJ CIO
Department IT Program Coordination Groups
Department Architecture Advisory Board
Chaired by:
Deputy CIO, Policy & Planning
ITIM Committee
Chaired by:
Asst. Director, Planning & Mgt
Policy and Planning Staff
E-Gov Committee
Chaired by:
Deputy Director,
E-Government Services
IT Security Council
Chaired by:
Deputy CIO, IT Security
Working Groups
Working Groups
Working Groups
Working Groups
Department of Justice – Office of the CIO

Figure 2-3. IT Governance Stakeholder Model - DOJ Oversight Groups

DOJ Office of the CIO (OCIO):

- **DOJ CIO.** The Department CIO is responsible for the acquisition and management of the Department's IT resources. The incumbent provides advice to the Deputy Attorney General and the Attorney General on all matters pertaining to IT.

- **DOJ OCIO Compliance Managers.** The DOJ OCIO compliance managers are staff members from each of the OCIO staffs responsible for one or more IT compliance review processes such as project management, enterprise architecture, security, privacy, etc. Compliance managers manage the review processes and ensure that the processes are integrated into the IT investment life cycle.

DOJ Partners:

- **DOJ Business Leaders.** These are the non-IT Department and Component executives and mission program managers who define mission and business priorities and rely on IT systems and services for the successful accomplishment of those missions and programs. The business leaders drive IT planning for the Department through the goals and objectives of the DOJ strategic plan and annual performance plan.
- **DOJ Chief Financial Officer (CFO).** The DOJ CFO participates in IT governance as a voting member of the DIRB and as the principal Department executive responsible to the Attorney General for overseeing the formulation and execution of the Department's budget.
- **DOJ Privacy and Civil Liberties Office (PCLO).** The DOJ Privacy and Civil Liberties Office is part of the Office of the Deputy Attorney General. The PCLOs mission is to protect the privacy and civil liberties of the American people by: reviewing and overseeing the Department's privacy operations; and ensuring the Department complies with Federal privacy statutes, including the Privacy Act of 1974. The PCLOs' primary role in IT governance is the review and approval of IT systems Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).
- **DOJ Budget Staff.** The DOJ Budget Staff, headed by the Chief Financial Officer (CFO), oversees the budget formulation process to prepare and submit the Department's budget to OMB and the Congress. IT investments represent a subset of the overall Department budget and it is through the annual budget data calls that IT investment requests are collected in OCIO and processed in partnership with the Budget Staff.

Component Partners:

- **Component Business Leaders.** The Component Business Leaders define the business priorities for each Component, collaborate with the Component CIO to select and prioritize IT investments during the Component's annual budget process and participate in the oversight of key Component investments to ensure acceptable results are achieved.
- **Component CIO.** The Component Chief Information Officer (CIO) is the senior IT manager within each Component responsible for overseeing the application and improvement of IT to support the Component's mission(s) and for verifying the accuracy of investment cost information. Though primarily responsible for the successful management of IT programs within their respective Components, Component CIOs also serve as members of the DOJ CIO Council, acting as advisors to the DOJ CIO on cross-Component issues ranging from IT policy and strategic planning to technology coordination.
- **Component Budget/Finance Staff.** The Component Budget/Finance Staff prepares and manages the Component's budget working closely with the Component ITIM Coordinator to ensure that IT budget information is accurately reflected within the Component's overall budget.

- **Component ITIM Coordinator.** The Component ITIM Coordinator acts as the liaison between the DOJ OCIO and the Component IT Project Managers to ensure completion of all Component ITIM activities and delivery of required Component ITIM products.
- **Component IT Project Manager.** The Component IT Project Manager provides reports and other information on their IT projects in response to Departmental data calls.

2.3.1 Integration Matrix

The Integration Matrix on the following page associates the IT governance stakeholders described on the preceding pages with the products and actions delivered throughout the IT Investment Life Cycle. The matrix helps link the flow of products between processes and from producers to users. Using the matrix, stakeholders can quickly determine the products or actions they must provide over the course of the IT Investment Life Cycle.

The matrix consists of three main elements: stakeholders, phases/processes and products/activities. The stakeholders are listed down the left-most column. The IT Investment Life Cycle phases and processes are shown sequentially across the top. Within the body of the matrix, the major products and actions for each process are listed in the column below the process name. The products and actions are listed in the cells corresponding to the stakeholder responsible for that product or action. By looking down each column, one can see all of the major products and actions delivered during a particular process and identify the stakeholder responsible for each product and action. Similarly, by looking across each stakeholder row, one can see all of the products and actions each stakeholder must deliver throughout the IT Investment Life Cycle.

IT Governance Integration Matrix - Processes, Stakeholders, & Products

	Life Cycle Years	Planning Year - 1	Planning Year				Budget Year		Operation Years	
	OMB ITIM Phases	Select Phase							Control - Evaluate Phases	
	IT Governance Phases	IT Planning Phase			IT Budget Phase				IT Oversight Phase	
	IT Governance Processes	IT Strategic Planning Process	EA Transition Planning Process	IT Investment Planning Process	Spring IT Budget Plng Process	Fall IT Budget Planning Process	OMB Passback IT Planning Process	Congressional Budget Planning Process	Executive Review Process	Compliance Review Process
STAKEHOLDERS										
Federal Oversight	Congress							- Enacted DOJ Appropriations Bill		
	OMB				- Draft Circular A-11 Updates	- Final Circular A-11 Updates - Ex. 300 Selection	- Passback Budget Decisions - Ex. 300 Review	- President's Budget		
	GAO									
	OIG									- Department Security Compliance Assessment
DOJ Partners	DOJ Business Leaders	- DOJ Strategic Business Needs, Changes, and Priorities								
	DOJ Budget				- Spring Budget Call - DOJ Spring Budget	- DAG Decisions - Fall Budget Call - DOJ Fall Budget	- OMB P/B Call - DOJ P/B Budget	- DOJ Responses to Budget Questions - DOJ Budget Spend Plan		
	DOJ PCLO									- Approves PIAs
DOJ Oversight	DIRB	- DOJ IT Strategic Plan Review			- DIRB-approved Spring IT Budget				- DIRB Review & Vote	
	CIO Council	- DOJ IT Strategic Plan Review								
	ITIM Committee				- Spring IT Budget Planning Support	- Fall IT Budget Planning Support				
DOJ CIO Office	DOJ CIO	- DOJ IT Strategic Goals		- DOJ IT Investment Priorities	- DOJ Spring IT Budget Recommendations		- DOJ P/B IT Budget Review	- CIO Responses to IT Budget Questions	- DIRB Project Selection	- CIO Project Dashboard Selections
	OCIO DIRB Exec Sec								- DIRB Meeting Summary - DIRB Action Reports	
	OCIO PPS-ITIM			- IT Investment Plan Data Call - DOJ IT Investment Plan	- Sprg IT Budget Call - IT Budget Trng - DOJ Sprg IT Budget	- Exhibit 300 Training - Fall IT Budget Call - DOJ Fall IT Budget - DOJ IT Capital Plan	- P/B Exec. Summary - P/B IT Budget Call - P/B IT Budget - Redacted Ex. 300s			
	OCIO PPS-EA	- DOJ IT Strategic Plan	- DOJ Transition & Sequencing Plan - IT Planning Guidance	- Investment EA Alignment Review	- Investment EA Compliance Ratings	- Exhibit 300 EA Review				- Department EA Compliance Reports
	OCIO ESS				- Investment C/S/R & PMQ Compliance Ratings	- Exhibit 300 C/S/R, PMQ & ACQ Reviews				- Department Project Compliance Reports
	OCIO EGSS				- Investment E-Gov & Privacy Compliance Ratings	- Exhibit 300 E-Gov & Privacy Reviews - PIA Review				- Department E-Gov & Privacy Compliance Reports
	OCIO ITSS				- Investment Security Compliance Ratings	- Exhibit 300 Security Review				- Department Security Compliance Reports
Component Partners	Component Business Leaders	- Component Strategic Business Needs, Changes, and Priorities								
	Component CIO	- Component Strategic IT Goals	- Component EA Transition Priorities	- Component IT Investment Priorities	- Component IT Budget Priorities					
	Component Budget/ Finance Staff				- Component Spring Exhibit 51/53	- Component Fall Exhibit 51/53	- Component Passback Exhibit 51/53	- Component Responses to Budget Questions		
	Component ITIM Coordinator			- Component IT Investment Plan	- Training RSVPs - Component Spring Exhibit 51/53	- Component Fall Exhibit 51/53 - Component PIAs & Exhibit 300s	- Comp. Passback Exhibit 51/53 - Component Exhibit 300 Updates	- Draft Component Responses to IT Budget Questions		
	Component IT Project Manager			- IT Investment Proposal	- IT Investment Budget Request	- Exhibit 300, if Required - PIA	- IT Investment Budget Update - Exhibit 300 Update	- Project Responses to IT Budget Questions	- DIRB Briefing	- Investment Compliance Reports

Figure 2-4. IT Governance Integration Matrix - Processes, Stakeholders and Products

2.4 System Development Life Cycle (SDLC) Framework

Chapter 2, paragraph 6b(1) of the Departments IRM Policy, DOJ Order 2880.1b establishes the DOJ CIO's authority to develop and implement department-wide program management guidelines, including a standardized System Development Life Cycle (SDLC) methodology. The Department's SDLC is a set of established procedures, practices and guidelines governing how DOJ information systems shall be planned, developed, implemented and managed until disposal. The Department's SDLC Guidance establishes standard processes and artifacts that:

- Allow for the orderly and effective development and implementation of IT systems.
- Provide visibility into the development process to permit independent assessment of program efforts and support investment management decisions.

The SDLC is for a single investment program what the Investment Life Cycle model is to the collection of investments that form the Department's IT portfolio. The SDLC consists of ten development life cycle phases that are described in detail in the Department's SDLC Guidance Document. The development life cycle phases are:

- Initiation
- Concept Development
- Planning
- Requirements Analysis
- Design
- Development
- Integration and Test
- Implementation
- Operations and Maintenance
- Disposition

During each of these phases, program teams may need to prepare a plan, perform a study, or complete a program evaluation or review before the program can proceed to the next phase. The plans, studies and evaluations prepared during system development help ensure that program teams perform the appropriate analysis and planning necessary to deliver the benefits expected from investments on time and within budget. These documents also serve as records of the decisions made during project planning, execution or evaluation for later reference.

Because of the wide variation in IT solutions, program scope, investment cost, risks, development approaches and implementation strategies that may be associated with an IT development project, program managers are given much discretion in tailoring the SDLC activities and artifacts for their assigned project. Depending upon the size, complexity and development approach of the program, life cycle phases may be combined or may overlap. However, to ensure that the essential planning and evaluation actions necessary for program success are performed and documented, the Department has identified a mandatory set of standard artifacts that must be prepared for all development and major enhancement programs.

All programs managed under the DOJ SDLC must prepare the artifacts listed in Figure 2-5. The purpose of each of these artifacts is described in the SDLC section listed in the 'Defined In' column. A template for each document can be found in the SDLC appendix listed in the 'Template' column. The 'Applicability' column designates the artifacts that are Mandatory or may be required As Directed. Other SDLC artifacts shall be prepared when appropriate.

The Lessons Learned Report (LLR) is the exception. Currently, the SDLC prescribes no standard format for the LLR. However, LLRs should contain at a minimum: (a) descriptions of techniques used to resolve the effects of unanticipated risks, (b) statements of effectiveness of management or development processes, (c) assessments of the effectiveness and impact of new or different technologies, and (d) details of any other experience that the program manager believes could increase the effectiveness of other programs. An LLR is required to close the Implementation phase and the Disposition phase. In some cases, Component or Department oversight authorities (e.g., program executives, Component CIOs, or the Department Investment Review Board (DIRB)) may direct the program manager to prepare a detailed Post Implementation Review (PIR) Report in lieu of the post implementation LLR.

Artifact Name	Defined In	Template	Applicability
Cost Benefit Analysis	SDLC 4.3.2	Appendix C-3	Mandatory
Risk Management Plan	SDLC 4.3.4	Appendix C-5	Mandatory
Concept of Operations Document	SDLC 5.1.11	Appendix C-9	Mandatory
Acquisition Plan	SDLC 5.3.1	Appendix C-6	Mandatory
Program Management Plan	SDLC 5.3.6	Appendix C-11	Mandatory
Functional Requirements Document	SDLC 6.3.1	Appendix C-14	Mandatory
Test and Evaluation Master Plan	SDLC 6.3.2	Appendix C-15	Mandatory
System Design Document	SDLC 7.3.3	Appendix C-19	Mandatory
Lessons Learned Report (LLR)	N/A	N/A	Mandatory
Post Implementation Review Report *	SDLC 10.1.5	Appendix C-34	As Directed*

* May be required in lieu of the Lessons Learned Report, as directed by Component or Department authority.

Figure 2-5. SDLC Minimum Deliverables

The artifacts listed in Figure 2-5 above are intended to (a) provide visibility into the decision making process for oversight and investment management assessments, (b) establish a minimum level of formal treatment of programmatic decisions, and (c) provide value to the programs by documenting requirements, management activities and acceptance criteria related to finished system capabilities. Programs may tailor these artifacts from the forms specified in the template appendices so long as the tailored products serve the basic artifact purpose described in the "Defined In" section of the SDLC guidance. For each tailored artifact, the program should document, via memorandum for the record, (a) the reason why tailoring occurred and (b) any foreseen impact of using a tailored template. These artifacts, when tailored, may be prepared as stand alone documents, or combined, if appropriate, so long as each SDLC artifact is clearly identified for future reference and location.

The SDLC deliverables identified in Figure 2-5 serve as a minimum compliance standard for DOJ programs. Program managers are highly encouraged to prepare other relevant deliverables defined in the SDLC. Over time, the DOJ OCIO may expand the list of mandatory and recommended SDLC deliverables in response to observed Departmental program development performance and to increase the use of best practices in program development activities.

There are three major stakeholders involved in applying and administering the Department's SDLC framework: the Department CIO, the Component CIO and the Program Manager. Their roles are as follows:

Department CIO:

- Establish an SDLC methodology and minimum requirements for compliance.
- Review SDLC artifacts, when appropriate, through the Department Executive and Compliance Review processes (Section 3.3) to monitor the performance of selected programs and systems.

Component CIO:

- Identify appropriate additional SDLC requirements for program visibility and control.
- Ensure Component programs comply with Department and Component SDLC requirements by reviewing artifacts, as necessary, during regular Component program oversight reviews (Section 2.7).

Program Manager:

- Identify all SDLC activities appropriate for the orderly and effective development and implementation of the IT system being developed and incorporate the activities into the program work plan.
- Ensure all required and necessary SDLC artifacts are prepared and maintained.
- Submit SDLC artifacts, when required, for Component and Department oversight reviews (Section 2.7).

To illustrate application of the SDLC guidance, consider how the guidance applies to the two example investments introduced earlier in this chapter.

> Investment A is an operational system undergoing a major enhancement of capabilities. The existing system is in O&M, therefore an initial set of SDLC artifacts is assumed to be in existence. The enhancement project is currently in the SDLC Design phase. Based on the mandatory artifacts listed in Figure 2-5, the program team must prepare or update the following artifacts for the enhancement effort before completing the Design phase:
>
> - Cost Benefit Analysis (update the cost benefit analysis for the enhancements)
> - Risk Management Plan (update to address the risks for the new work)
> - Concept of Operations (CONOPS) (incorporate the new capabilities)
> - Acquisition Plan (describe how the contract(s) for the new work will be awarded)
> - Program Management Plan (update to address management of the new work)
>
> Investment B is a new program in the Development phase. Per Figure 2-5, the program team must prepare the following artifacts before beginning development:
>
> - Cost Benefit Analysis
> - Risk Management Plan

- Concept of Operations (CONOPS)
- Acquisition Plan
- Program Management Plan
- Functional Requirements Document
- Test and Evaluation Master Plan
- System Design Document

For more information on the DOJ SDLC, please visit the DOJ SDLC website at: http://www.usdoj.gov/jmd/irm/lifecycle/table.htm

2.5 Enterprise Performance Management (EPM)

The purpose of Enterprise Performance Management (EPM) is to provide a standard method for measuring the Department's progress toward its target state using a set of performance metrics consistent with an investment's purpose and its position in the SDLC. EPM is results oriented, and shows a causal relationship between the performance of individual IT investments and the success of the Department as a whole. This approach helps provide rigor and due diligence to the IT Governance Framework and the IT Investment Life Cycle, and helps to ensure that investments such as our example Investments A and B deliver the strategic and business needs that they are intended to provide

Performance measurement is a cyclical process that begins with defining strategic needs and envisioning desired outcomes. The process is continued by assessing current performance and performance gaps, establishing target improvements and measures of success, measuring results and comparing results to targets. The process is reiterated by establishing new targets and identifying actions necessary to achieve those targets. This cycle is illustrated by the Enterprise Performance Management (EPM) model shown in Figure 2-6. The EPM model provides a methodology for continually improving an investment's performance through periodic review and analysis of investment results. This approach enables DOJ leadership to take into account how IT investments contribute to the success of the Department's priorities when making budget decisions and to take corrective action when necessary.

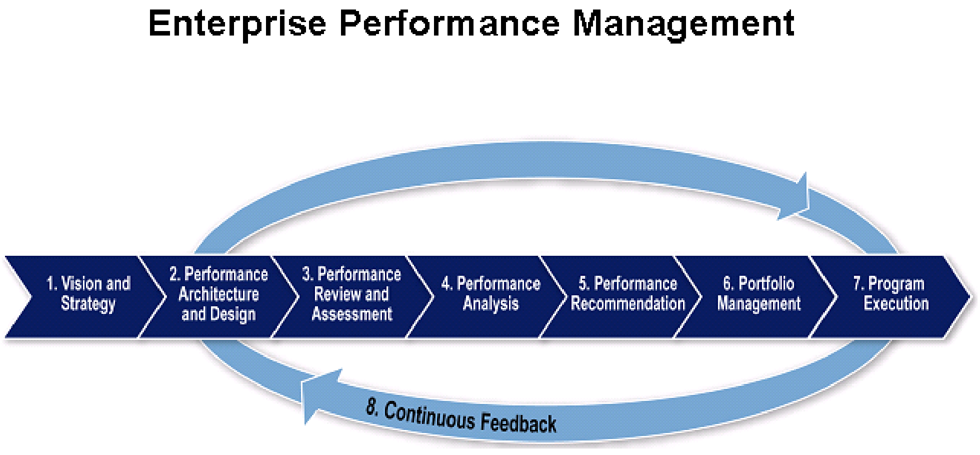

Enterprise Performance Management
1. Vision and Strategy
2. Performance Architecture and Design
3. Performance Review and Assessment
4. Performance Analysis
5. Performance Recommendation
6. Portfolio Management
7. Program Execution
8. Continuous Feedback

Figure 2-6. Enterprise Performance Management

The eight EPM stages link to the activities of the IT Investment Life Cycle as described below.

1) In the Vision and Strategy stage, the Department's Strategic Goals and Priorities from the DOJ Strategic Plan and IT Strategic Plan provide direction for designing, developing and aligning the Enterprise Performance Architecture.
2) In the Performance Architecture and Design stage, the EAPMO identifies program and mission performance goals and metrics, aligns them to the Department's Segment Architectures and selects key IT performance metrics to measure achievement of segment goals. The PAR and PART are the key sources for mission performance measurement metrics.
3) In the Performance Review and Assessment stage, individual investment performance results are gathered, compared to performance goals and aggregated into Segment performance results.
4) In the Performance Analysis stage, the EAPMO reviews the Department's Segment performance metrics in relation to investment specific performance results and identifies performance gaps / issues for each Segment.
5) Performance Recommendations are developed to address performance gaps discovered during Performance Analysis and help shape investment priorities for the IT Investment Planning Process.
6) In the Portfolio Management stage, the Performance Recommendations are used to inform investment selection decisions in the IT Budget Phase to shape the Department's IT portfolio.
7) In the Program Execution stage, investment managers monitor investment performance results during the IT Oversight Phase.
8) Through Continuous Feedback, performance results collected for oversight reviews are compared against the performance targets in the Performance Architecture to start the next IT planning cycle.

The Department's EPM process is being integrated into the Department's annual ITIM process in order to gather investment performance information on a regular basis. The process is being implemented incrementally beginning with a limited set of key investments. These investments will be selected from investments that are monitored by the DIRB, reported on the OCIO Project Dashboard, and included in the DOJ Transition Strategy and Sequencing Plan.

The DOJ EAPMO will analyze the performance metrics for the initial set of investments to establish a causal line of sight between investment performance and overall Segment and Department performance. To align performance measurement across the Department, the DOJ EAPMO is developing guidance for development and selection of program/investment performance metrics. Components will apply the guidance to determine investment metrics. The DOJ EAPMO will review the metrics selected and provide feedback to the Components to improve or align the metrics for consistent measurement across the Department. At least one metric in each of the following four categories will be captured for each investment:

- **Technology Metrics** that measure the performance of systems;
- **Process and Activity Metrics** that measure the activities that occur

- **Business Outcome Metrics** that measure the success of a customer or business results; and,
- **Information Sharing Metrics** that measure how the investment shares information across the Department and with other stakeholders.

The DOJ EAPMO will collect performance information on a semi-annual basis. This will allow programs to set their performance targets at the beginning of the fiscal year and report on their progress at mid-year and year end. To implement the EPM process, the focus of the effort for FY08 is to identify the initial set of key investments and to collect and define the performance metrics for those investments. Key responsibilities for Department, Component and Program stakeholders are highlighted below.

Key Department-level responsibilities:

- The DOJ EAPMO is responsible for developing Guidance on the types of metrics that should be developed and reported for programs/investments. This includes the development of a Metrics Catalogue of the different types of metrics and measures being gathered across the Department.
- The DOJ EAPMO will normalize the individual program/investment metrics so that similar metrics are used across the Department.

Key Component-level responsibilities:

- Components are responsible for ensuring that performance metrics are developed for Component programs/investments, and that the metrics are tracked and reported to the Department periodically, as requested.

Key Program-level responsibilities:

- Program Managers must develop performance metrics and track performance results for the program/investment that they manage.

The DOJ EAPMO will use the Department's Segment Architecture to group investments and activities into manageable pieces for performance analysis. The results of the analysis will be used to help the Department manage its IT resources and to focus those resources on the continued development and employment of Enterprise Solutions. Using the EA Segments, performance metrics from the various Components and programs will be grouped to provide a broader picture of the Department's success in delivering the strategic outcomes for particular mission areas. Analyzing performance using the Segment Architecture helps to relate the successful delivery of IT investments to success in delivering the Department's strategic goals and missions.

In the terms of our example, both Investment A and B's annual outcomes / results will be measured against their roles in fulfilling mission / business needs by applying Segment Architecture using the PAR and other applicable performance metrics. Such metrics may include the investments classification (discussed further in Section 2.6) and / or current position in its SDLC. After performance results are reviewed and analyzed, recommendations can be made for improving each investment to better meet the strategic / business need it was created to address.

In addition to the segment grouping of performance measures provided by the segment architecture approach, the DOJ EAPMO is identifying outcome-focused performance metrics for use by specific IT investments and is working to standardize performance metrics across the department. These metrics and progress measurements will be integrated into the DOJ CIO Project Dashboard that tracks EVM progress of major investments. (See Section 3.3.2.7 for more information on Cost / Schedule / Risk Compliance Review, including the DOJ CIO Project Dashboard.)

For more information on the Enterprise Performance Model, refer to the DOJ Performance Architecture Document v.3 which is available from the Department OCIO EA PMO.

2.6 Investment Classification Model

The Investment Classification Model provides a structure for classifying investments to support portfolio analysis and to determine the oversight reviews required for each investment at any point in its life cycle. Investments are classified in three tiers: scope of the investment, the type of technology investment and the life cycle stage of the investment.

1. The first tier of investment classification supports the Department's strategic goal of unifying / standardizing solutions across the IT enterprise by identifying the planned scope of an investment and the users the investment is intended to help. All investments are classified as either Enterprise Investments or Component Investments. Investments intended to fill a single Component's business needs are classified as Component Investments, whereas investments intended to fill the needs of multiple Components are classified as Enterprise Investments. Each Enterprise Investment will be assigned to a lead Component that is responsible for ensuring that the appropriate compliance reviews are completed. For the purpose of classification, the following definitions are used:

    a. **Enterprise Investment.** An investment that supports the functional needs of two or more Components.
    b. **Component Investment.** An investment that supports the functional needs of a single Component.

2. The second tier of investment classification supports the Department's strategic goal of reducing redundant infrastructure by identifying the type of business need an investment is meant to fulfill. Using the categories in the Department's definition of IT (See Section 1.2 and Appendix B.), each investment is classified as a Mission-Delivery and Business Solution, Infrastructure, or IT Practices and Management investment. Investments that are a mix of two or more of these types are apportioned to each category based on the percentage of funding applied in each area. For the purposes of classification, apportionment and IT cost reporting the following definitions are used:

a. **Mission-Delivery and Business Solutions.** The software applications, systems, services and the people, processes, commercial contracts, overhead occupancy and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department. Mission-Delivery and Business Solutions provide support for the missions of the Department as stated in the DOJ Strategic Plan.

b. **Infrastructure.** The people, processes, commercial contracts, overhead occupancy and technology used to interconnect computers and users and automate business processes. Infrastructure is also used to acquire, process, store, send, receive, interchange, manage, switch, transmit, electronic data and information. Infrastructure is further classified into three sub-classes, consistent with the IT Infrastructure Line of Business categories established by OMB: End User Systems & Support; Mainframe & Server Systems & Support; and Telecommunications Systems & Support. These sub-classes are defined as follows:

   I. **End User Systems & Support**. Includes the people, processes, commercial contracts, overhead occupancy and technology necessary to enable and support an end user in their interaction with information technology services.

   II. **Mainframe & Server Systems & Support**. Includes the people, processes, commercial contracts, overhead occupancy and technology to provide physical or logical, centralized or aggregated computer systems and related services to one or more parts of the enterprise(s).

   III. **Telecommunications Systems & Support**. Includes the people, processes, commercial contracts, overhead occupancy and technology to provide any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.

c. **IT Practices and Management.** The programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support **<u>all</u>** the IT investments of the component.

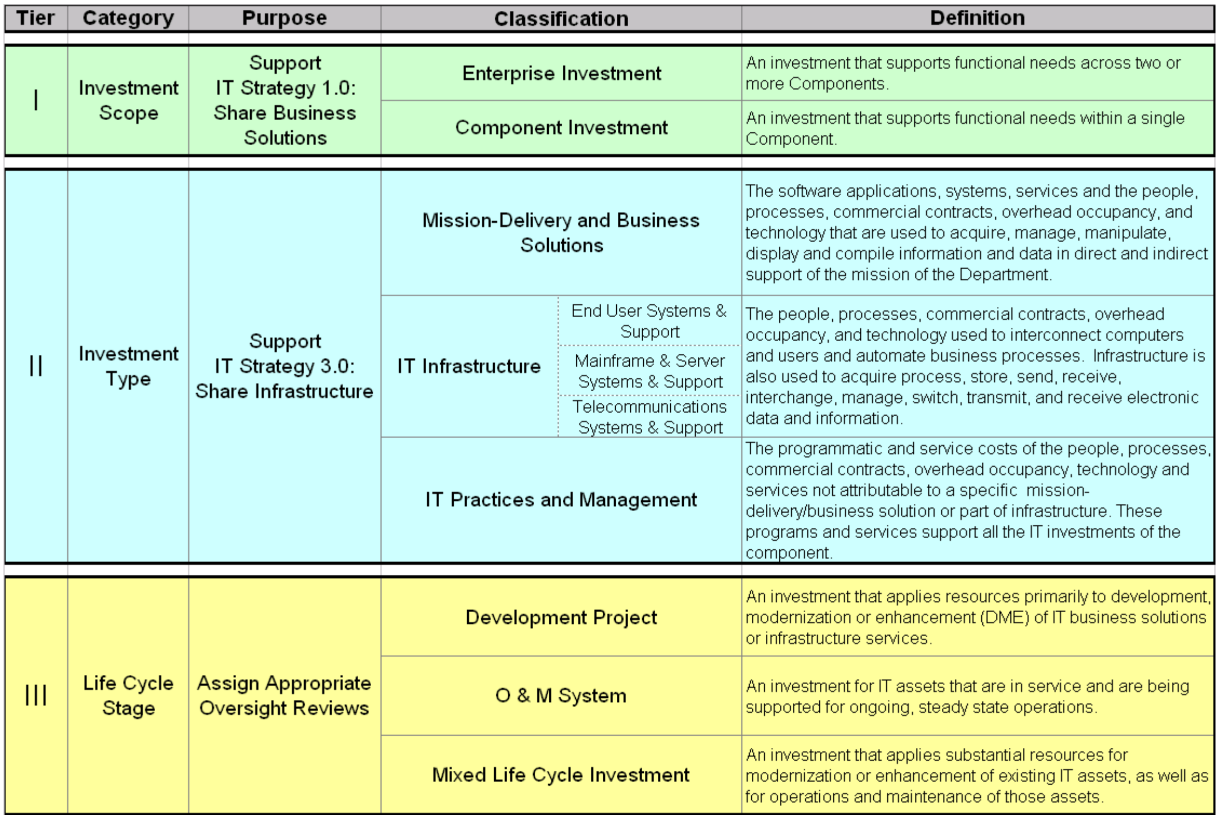
3. The third tier of investment classification identifies the investment's life cycle stage and is used to determine the appropriate oversight reviews that are required. IT investments are classified as development projects, operations and maintenance (O&M) systems, or mixed life cycle investments. Investments that are classified as mixed life cycle investments are apportioned to development and O&M based on the amount of funding applied in each area. For the purposes of classification and apportionment, the following definitions are used:

a. **Development Projects.** Development projects are investments that apply substantial resources to development, modernization or enhancement (DME) of IT business solutions or infrastructure services[2]. Projects have start and end dates and deliver an IT asset or service when completed. Development project investments fund the activities for planning, developing, testing, or implementing new infrastructure or business solutions, expanding existing solutions to serve new users and uses, or implementing significant enhancements to existing infrastructure or business solutions to update or improve existing capability(ies).

b. **Operations and Maintenance (O&M) Systems.** O&M systems are assets that are in service and are being supported for ongoing operations[3]. While there is often some low level of ongoing system enhancement, the new work is usually to maintain system performance or operational availability.

c. **Mixed Life Cycle Investments.** Mixed life cycle investments are investments that apply resources for significant modernization or enhancement of existing IT assets, as well as for the ongoing operations and maintenance of those assets.

The relationship of these three classification tiers is illustrated in the Investment Classification Model in Figure 2-7. Using these three classification tiers, the Department's IT portfolio's costs can be grouped and analyzed for strategic, investment and budget planning.



Tier	Category	Purpose	Classification		Definition
I	Investment Scope	Support IT Strategy 1.0: Share Business Solutions	Enterprise Investment		An investment that supports functional needs across two or more Components.
			Component Investment		An investment that supports functional needs within a single Component.
II	Investment Type	Support IT Strategy 3.0: Share Infrastructure	Mission-Delivery and Business Solutions		The software applications, systems, services and the people, processes, commercial contracts, overhead occupancy, and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department.
			IT Infrastructure	End User Systems & Support	The people, processes, commercial contracts, overhead occupancy, and technology used to interconnect computers and users and automate business processes. Infrastructure is also used to acquire process, store, send, receive, interchange, manage, switch, transmit, and receive electronic data and information.
				Mainframe & Server Systems & Support	
				Telecommunications Systems & Support	
			IT Practices and Management		The programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support all the IT investments of the component.
III	Life Cycle Stage	Assign Appropriate Oversight Reviews	Development Project		An investment that applies resources primarily to development, modernization or enhancement (DME) of IT business solutions or infrastructure services.
			O & M System		An investment for IT assets that are in service and are being supported for ongoing, steady state operations.
			Mixed Life Cycle Investment		An investment that applies substantial resources for modernization or enhancement of existing IT assets, as well as for operations and maintenance of those assets.

Figure 2-7. Investment Classification Model

[2] Investments for technical refresh of systems are considered development projects that may require project reviews.

[3] Operations and maintenance investments may contain nominal funds for development, as long as the development activity does not rise to the level of requiring a Component or Department-level project review. When the development activity is significant enough to require project review, the investment will typically be classified as a Project for the purpose of review.

To illustrate how the Investment Classification Model is used, the three classification tiers are applied to the two example investments introduced at the beginning of this chapter.

Investment A is classified as an Enterprise Business Solution Mixed Life Cycle investment for the following reasons:

- Enterprise - It fulfills a business need for two or more Components.
- Business Solution – It is an application that directly supports a business function.
- Mixed Life Cycle – It is in O&M, but is undergoing a major enhancement.

Because Investment A is an Enterprise Business Solution, it will likely receive a high priority ranking in the Department IT portfolio during investment and budget planning.

Investment B is classified as a Component Business Solution Development project for the following reasons:

- Component – It fulfills the mission or business needs of a single Component.
- Business Solution – It is an application that supports a specific business function.
- Development Project – It is under development and is not yet operational.

Because Investment B is a Component Business Solution, the managing Component must strongly justify the investment's priority during investment and budget planning.

2.7 IT Oversight Model

The IT Oversight Model communicates the Department's vision for integrating the processes and products of the IT Oversight Phase of the IT Investment Life Cycle based on the investment's position in the SDLC and its classification. The model provides a structure for describing the levels of oversight that occur at the Department and in the Component CIO offices.

Oversight of IT investments should serve two main purposes:

- Monitor the progress and performance of projects and other investments to ensure they are managed well and deliver expected results.
- Provide feedback to influence resource planning decisions for the future.

To accomplish these purposes while enabling the Department to allocate limited oversight resources across the IT portfolio, oversight reviews occur at two levels – the Department and the Component.

- **Department Reviews.** Monitor investments that are high cost, high risk, or high visibility, investments that are important to Department-wide missions or cross-government integration, or ensure uniform compliance with Federal and Department policies and procedures.
- **Component Reviews.** Monitor the progress of development projects and O&M systems important for Component success and assess investment performance and compliance with Component business practices, processes and procedures.

There are two primary types of Department and Component oversight reviews – Executive Reviews and Compliance Reviews.

- **Executive Reviews.** These reviews are performed by executive oversight groups to ensure that investments are aligned with the Department's and/or Component's strategic priorities (respectively) and to ensure that key investments are delivering the business value and return on investment (ROI) commensurate with investment costs.
- **Compliance Reviews.** These reviews are typically performed by functional oversight groups to ensure that projects and other investments proceed according to approved plans, deliver expected service, and comply with established policies, procedures and standards.

Executive and Compliance reviews are divided into two groups, based on the life cycle stage of the investments being reviewed – Project Reviews and O&M Reviews.

- **Project Reviews.** Regular or event-driven reviews that monitor the progress of development projects against cost targets, schedule milestones and completion of compliance requirements associated with design, development or implementation. Project reviews typically occur on a frequent basis, such as monthly or quarterly, to monitor progress. Project reviews may also occur at key milestones in the project life cycle when decisions are required to move the project from one SDLC stage to another.
- **O&M Reviews.** Periodic reviews that assess operational systems for effectiveness, cost management, customer satisfaction and compliance with established operating procedures and management standards. O&M reviews are typically performed annually.

To share the results of compliance reviews beyond the oversight process, the Department compliance managers provide input to a consolidated Compliance Report.

- **Compliance Report.** Provides a Yes/No recommendation from oversight Compliance Managers to inform IT planners and senior executives of serious compliance issues associated with specific investments. The report is primarily used during IT planning and budget review.

The IT Oversight Model in Figure 2-8 illustrates how the oversight processes, products and stakeholders work together to achieve the two purposes of oversight. The model contains three types of elements:

- IT governance phases - shown in blue. The phases shown are the OMB Select and Control/Evaluate Phases and the Department IT Planning phases.
- Oversight reviews - shown in green. The Department and Component Executive and Compliance Reviews are shown.
- Products - shown in white. These are the OMB reports, compliance reports and investment priorities.

The model illustrates the individual compliance reviews performed at the Department and Component levels, as well as the IT planning processes that use the compliance reports. This view also identifies which compliance reviews apply to Projects and O&M systems.

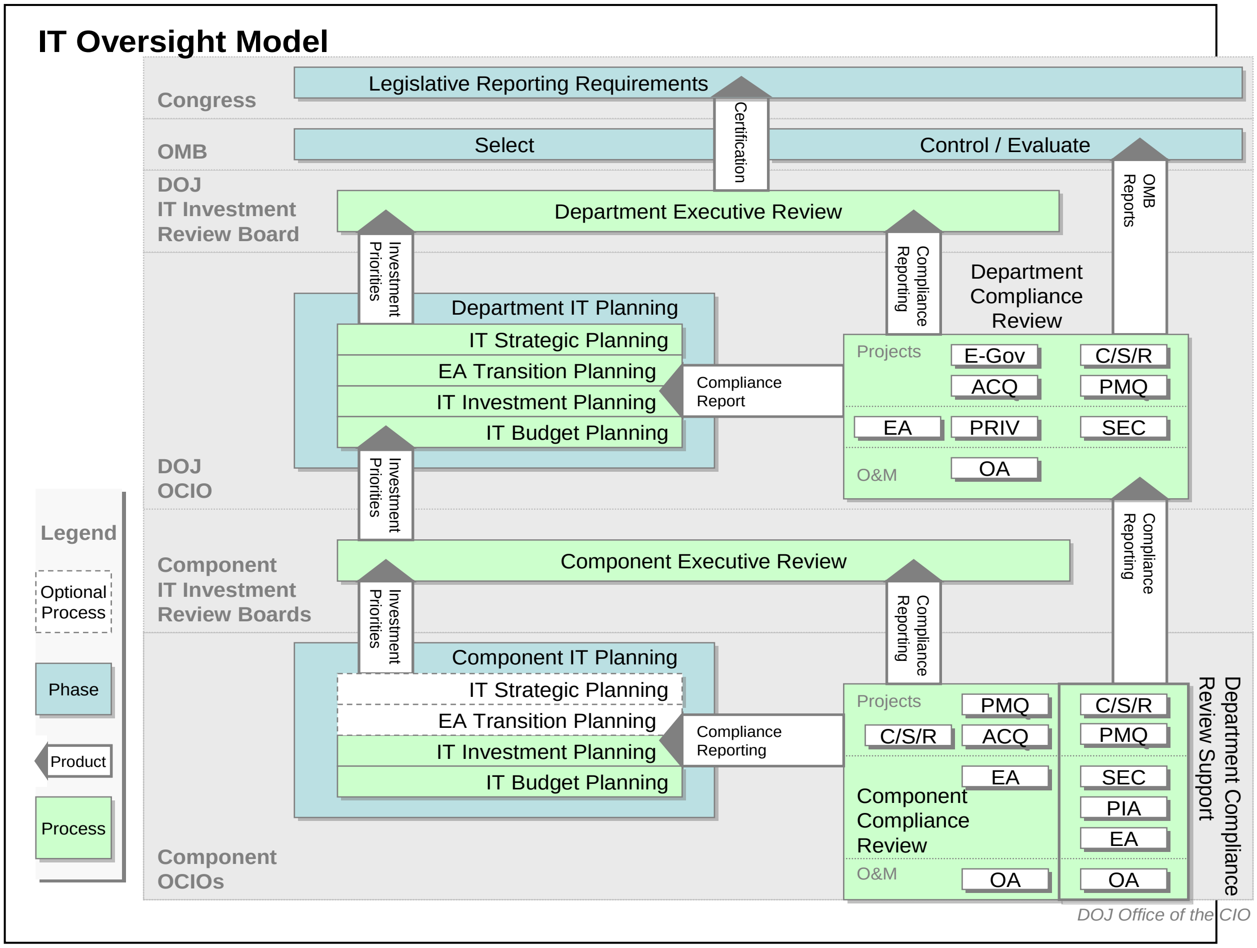


Figure 2-8. IT Oversight Model

The Department Executive Review serves three purposes:

- Prioritizes investments for the IT budget during the Select Phase.
- Oversees the progress and management of selected Department-level projects in the Control/Evaluate Phase.
- Certifies that appropriate project oversight mechanisms are in place for specified investments.

The Department Compliance Review serves three purposes:

- Ensures IT projects are complying with Departmental and Federal standards and regulations.
- Produces compliance reports required by OMB.
- Provides information for the Compliance Report used in Department IT planning.

The Department Compliance Review process consists of eight compliance reviews that are described in the text box to the right.

Four of these reviews only apply to projects:

- Project Manager Certification Review
- Acquisition Review
- E-Gov Review
- Cost/Schedule/Risk Review

One review only applies to O&M and mixed life cycle systems:

- Operational Analysis Review

These three remaining reviews apply to both projects and O&M systems:

- Enterprise Architecture Review
- Security Review
- Privacy Review

The Component portion of the IT Oversight Model looks very similar to the Department portion, with one key difference: Component compliance review responsibilities are divided between Department Compliance Review Support and Component Compliance Review.

This division of compliance review responsibilities recognizes that Components not only provide information needed for compliance reviews performed at the Department-level, they also perform compliance reviews at the Component-level and use the results of those reviews internally to satisfy Component IT planning and oversight needs.

Compliance Reviews

Project Management Qualification (PMQ) Review. Reviews the qualifications of project managers for compliance with the Federal IT Project Manager Guidance from the Federal CIO Council.

Enterprise Architecture (EA) Review. Reviews alignment of investments to segment architectures to prevent duplication and to identify opportunities for consolidation or standardization of technologies or services.

Acquisition (ACQ) Review. Reviews software and support service procurements for compliance with government-wide acquisition regulations and use of Federal or Department-wide software license and support service blanket purchase agreements.

E-Government (E-Gov) Review. Reviews investments identified as part of the Department's E-Government Implementation Plan for completion of OMB-approved milestones.

Security (Sec) Review. Reviews all systems and applications for compliance with Federal and Department IT security policies and specifications.

Privacy (PIA) Review. Monitors the preparation, approval and posting of Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) for compliance with OMB and DOJ privacy policies.

Cost/Schedule/Risk (C/S/R) Review. Reviews development projects to ensure acceptable progress toward on-budget and on-time delivery and effective management of project risks.

Operational Analysis (OA) Review. Reviews selected high cost O&M investments to ensure they continue to effectively deliver their operational goal(s) and meet approved cost targets.

The Component Executive Review serves two purposes:

- Prioritizes Component investments for Component and Department IT planning.
- Monitors the progress of selected Component-level investments in the Control and Evaluate phases.

Component responsibilities for Department Compliance Review Support consist of providing Cost/Schedule/Risk, Project Manager Qualification, Security, Privacy, EA and OA reports for projects and O&M systems as directed by Department Compliance Managers.

Component responsibilities for Component-level Compliance Reviews consist of performing three types of reviews for projects – Cost/Schedule/Risk, Project Manager Qualification and Acquisition – and one review – Operational Analysis – for O&M systems. Components are responsible for conducting EA reviews of development Projects and O&M systems to ensure compatibility. The compliance information produced from the Component Compliance Reviews should be used as input to Component IT Planning and IT Budget Planning processes. Additional guidance for Component oversight is provided in the following section that discusses the Component Self-governance Model.

To illustrate how the IT Oversight Model is used, the model is applied to the two example investments introduced at the beginning of this chapter.

Investment A is classified as an Enterprise Business Solution Mixed Life Cycle investment. Consequently, the investment is subject to the following reviews:

- Department Executive Review because it is an Enterprise Investment undergoing a major enhancement.
- Department Compliance Reviews for projects and O&M systems as specified by the selection criteria for each Department Compliance Review. (Specific selection criteria are defined in Section 3.3.2.)
- Component Compliance Reviews as specified by Component oversight processes and selection criteria.

Investment B is classified as a Component Business Solution Development Project and is therefore is subject to the following reviews:

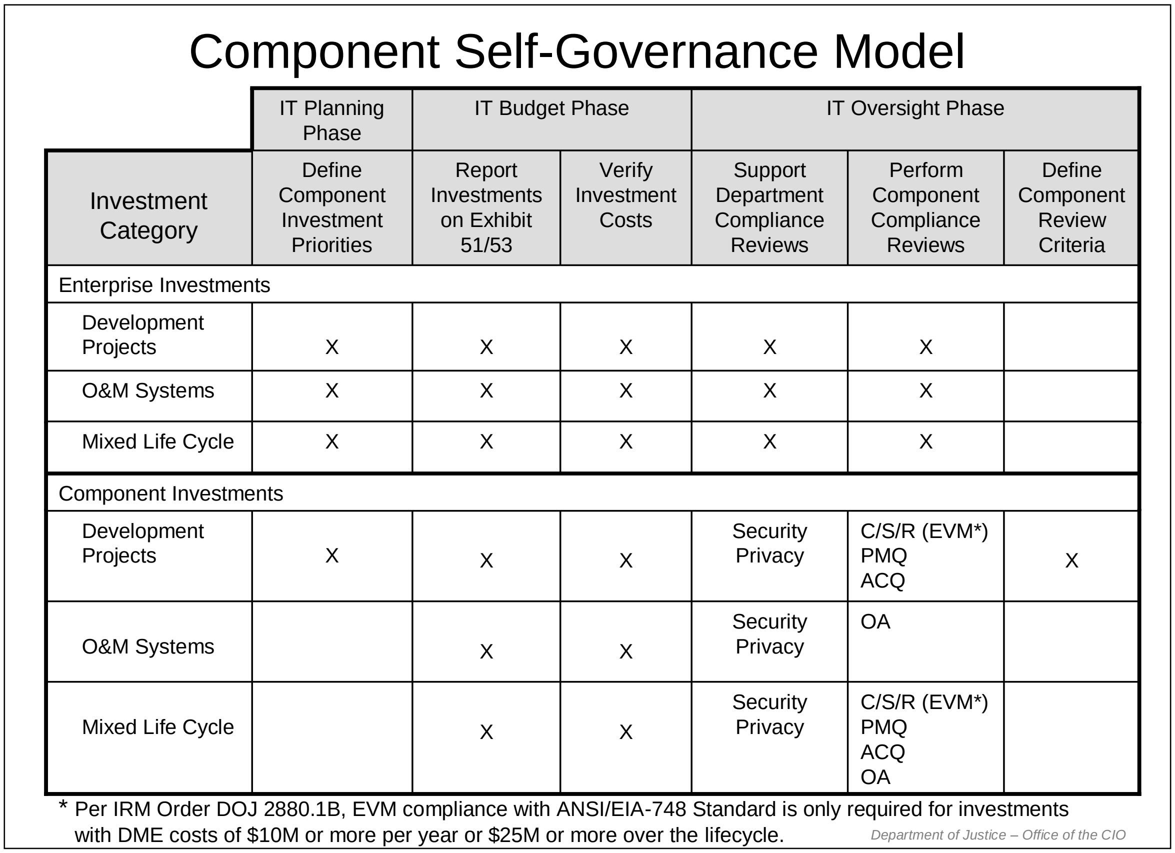
- Department Compliance Reviews for Security and Privacy that apply to all Component and Department projects and O&M systems. (Specific selection criteria are defined in Section 3.3.2.)
- Component Compliance Reviews as specified by Component oversight processes and selection criteria.

2.8 Component Self-Governance Model

One of the purposes of this Guide is to communicate to the Component CIOs the Department's expectations for Component self-governance. The OCIO developed the Component Self-Governance Model to help Components identify the requirements for self-governance actions to the IT Budget and IT Oversight Phases and to help them implement the specific requirements for internal Component IT governance.

By applying the investment classifications defined in the Investment Classification Model, Components can discern the specific actions they must plan to perform throughout the Investment Life Cycle for both Component investments and Enterprise investments for which they are the managing Component.

The Component Self-Governance Model in Figure 2-9 applies the categories from the Investment Classification Model described in Section 2.6 to show when Component Self-governance must be performed during the Investment Life Cycle for each investment type[4].



Component Self-Governance Model

	IT Planning Phase	IT Budget Phase		IT Oversight Phase		
Investment Category	Define Component Investment Priorities	Report Investments on Exhibit 51/53	Verify Investment Costs	Support Department Compliance Reviews	Perform Component Compliance Reviews	Define Component Review Criteria
Enterprise Investments						
Development Projects	X	X	X	X	X	
O&M Systems	X	X	X	X	X	
Mixed Life Cycle	X	X	X	X	X	
Component Investments						
Development Projects	X	X	X	Security Privacy	C/S/R (EVM*) PMQ ACQ	X
O&M Systems		X	X	Security Privacy	OA	
Mixed Life Cycle		X	X	Security Privacy	C/S/R (EVM*) PMQ ACQ OA	

* Per IRM Order DOJ 2880.1B, EVM compliance with ANSI/EIA-748 Standard is only required for investments with DME costs of $10M or more per year or $25M or more over the lifecycle.

Department of Justice – Office of the CIO

Figure 2-9. Component Self-Governance Model

[4] Components that do not directly manage IT services or investments have no obligation to implement IT self-governance processes and are not included in the process discussions in Section 3.

Six primary Component self-governance actions are required to support Department-level processes during the three IT governance life cycle phases. Those actions are:

IT Planning Phase action:

- Define Component Investment Priorities

IT Budget Phase actions:

- Report Investments on Exhibit 51/53
- Verify Accuracy of Investment Costs

IT Oversight Phase actions:

- Support Department Compliance Reviews
- Perform Component Compliance Reviews
- Define Component Review Criteria

To illustrate how the Component Self-governance Model is used, the model is applied to the two example investments described earlier.

Investment A is a Mixed Life Cycle Enterprise investment that is required to undergo Department-level reviews. Per the model, the managing Component responsibilities are:

- Report the investment in its investment priorities during the IT Planning Phase.
- Report the investment on Exhibit 51/53 and verify the investment cost during the IT Budget Phase.
- Support all appropriate Department Compliance Reviews in the IT Oversight Phase.
- Perform appropriate Component-level Compliance Reviews to ensure that the investment will be delivered on time, on budget and to specifications.

Investment B is a Component investment and is primarily reviewed at the Component level. Per the model, the Component responsibilities for this investment are:

- Report the investment in its investment priorities during the IT Planning Phase.
- Report the investment on Exhibit 51/53 and verify the investment cost during the IT Budget Phase.
- Support Department Security and Privacy Compliance Reviews in the IT Oversight Phase.
- Perform appropriate Component-level Compliance Reviews to ensure that the investment will be delivered on time, on budget and to specifications.

Specific Component self-governance actions required to support the Department’s governance processes are described in a text box titled *Component Self-Governance* at the end of each process description in Section 3.

3. Governance Phases and Processes

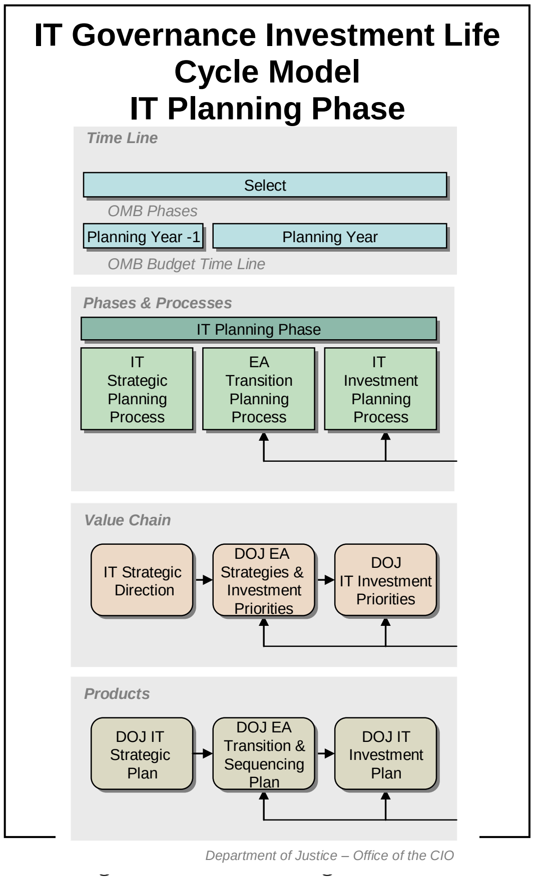
The IT Governance Investment Life Cycle Model, introduced in Section 2.2 of this Guide, provides the framework for the processes that are discussed in this section. The model portrays the end-to-end processing needs for the Department's IT governance. It contains three sequential life cycle phases for IT planning, budgeting and oversight and each phase contains two or more governance processes. In this section, each phase is briefly reintroduced to provide context, followed by a detailed discussion of each process in the phase.

Each process is discussed in three parts.

1. The first part contains a brief discussion of the high-level activities in the process, a summary diagram depicting the sequence of the high-level activities and a definition of the resulting product(s).
2. The second part provides expanded detail on the workings of the process. It contains a process diagram that depicts the flow of lower-level subprocesses and shows stakeholder involvement through the use of swim lanes. For each lower-level subprocess, a brief description is provided.
3. The third part describes the Department's requirements for Component self-governance. For some processes, the Department requires Components to perform like or similar processes within their Components.

3.1 IT Planning Phase

The first phase of the governance life cycle is the IT Planning Phase. It begins with strategic planning that defines the Department's strategic goals and priorities and culminates with IT investment planning that produces the IT Investment Plan used to guide IT budget decisions.


IT Governance Investment Life Cycle Model
IT Planning Phase
Time Line
Select
OMB Phases
Planning Year -1
Planning Year
OMB Budget Time Line
Phases & Processes
IT Planning Phase
IT Strategic Planning Process
EA Transition Planning Process
IT Investment Planning Process
Value Chain
IT Strategic Direction
DOJ EA Strategies & Investment Priorities
DOJ IT Investment Priorities
Products
DOJ IT Strategic Plan
DOJ EA Transition & Sequencing Plan
DOJ IT Investment Plan
Department of Justice – Office of the CIO

The IT Planning Phase spans approximately thirteen months from March through March and consists of three major planning processes, each generating one key Department-level planning document.

1. The DOJ IT Strategic Planning Process generates the Department's IT Strategic Plan.

2. The DOJ EA Transition Planning Process generates the Department's EA Transition Strategy and Sequencing Plan.

3. The DOJ IT Investment Planning Process produces the Department's IT Investment Plan.

The IT Planning Phase is designed to transform the mission and business drivers from the Department's Strategic Plan into a prioritized investment plan to guide the formulation of the Department's IT budget. The following sections describe the IT Planning Phase processes that produce the Department's IT plans, summarize the contents of the process outputs, identify the responsibilities of the process stakeholders and specify the associated requirements for Component self-governance.

3.1.1 IT Strategic Planning Process

In the IT Strategic Planning Process, the DOJ OCIO examines the current state of the Department's IT enterprise and its support of Department missions and objectives; determines the defines IT strategic goals and programs; assigns priorities, performance goals, indicators and metrics; and produces the Department's IT Strategic Plan. The DOJ IT Strategic Plan provides the Department CIO's vision and strategic goals for evolving the IT program to more effectively enable Department mission goals and objectives. The plan covers a 3-5 year period and drives the Department's enterprise architecture and IT capital planning. The plan identifies business and mission challenges that face the Department, the key mission and technology drivers that act on the IT strategy and ultimately the key strategies, programs and actions that the Department will undertake to respond to these challenges. Since the plan covers a multi-year period, a new plan is not developed every year; however, the plan is reviewed annually to determine if updates are needed to keep the plan current. While minor updates to the plan may be made every year, major plan revisions are expected to occur roughly in conjunction with the induction of each new administration.

To begin the process, the OCIO staff examines the Department's Strategic Plan and strategic goals and confers with the Department's business leadership to understand their business priorities, emerging needs and any potential changes looming on the horizon. The Department Deputy CIOs are also consulted to identify critical IT strategic priorities. The first draft of the plan is developed by the OCIO staff to address each of the CIO's major responsibilities. The individual Deputy CIO staffs review the initial draft and appropriate adjustments are made. During this process, the major Department program offices as well as Component CIO staffs are consulted to identify Component strategic priorities. Following the staff review, each Deputy CIO conducts a final review to concur with the working draft. Throughout this process, regular briefings are held with the CIO to insure that the plan reflects his/her priorities and goals. Once a final working draft of the plan is concurred with by the Deputy CIOs, formal reviews are conducted with the Department business leadership, the DOJ CIO Council and the Department IT Investment Review Board (DIRB) to produce the final document. Once the final IT Strategic Plan is formally approved by both the DOJ CIO Council and the DIRB, the plan is presented to the Deputy Attorney General for approval and is published and released.

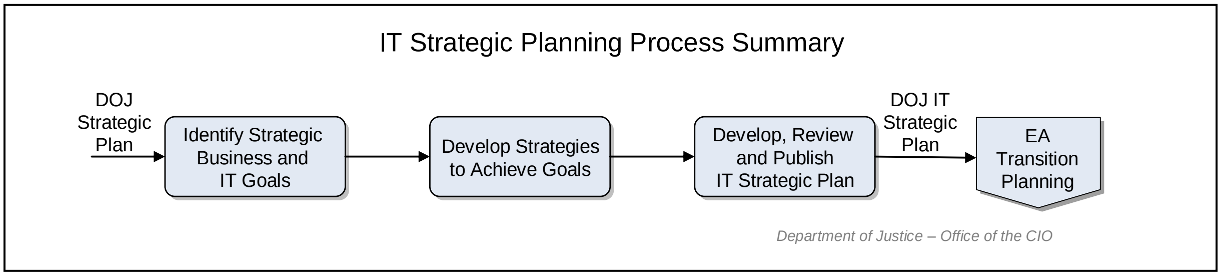
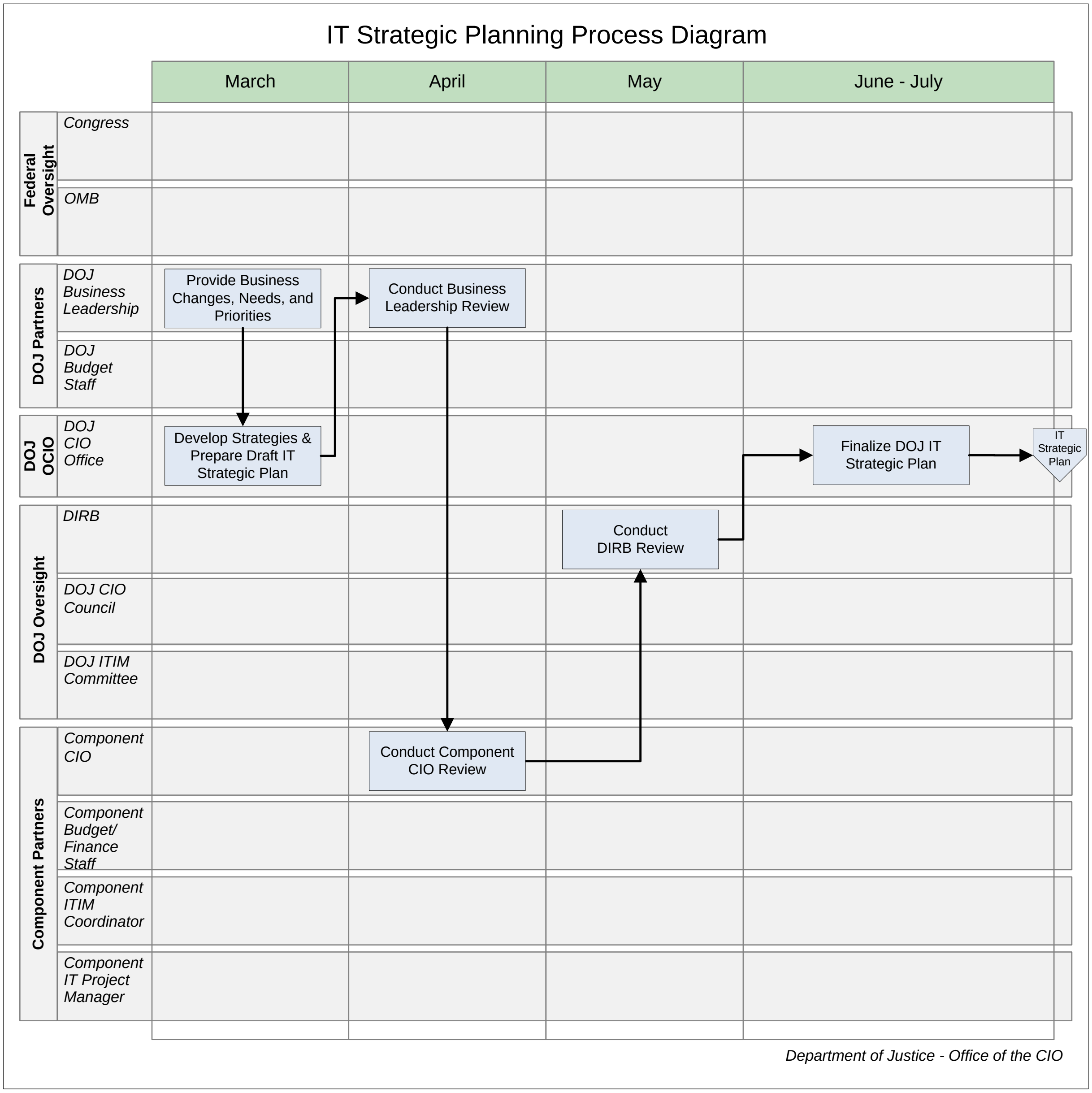

IT Strategic Planning Process Summary
DOJ
Strategic
Plan
Identify Strategic Business and IT Goals
Develop Strategies to Achieve Goals
Develop, Review and Publish IT Strategic Plan
DOJ IT
Strategic
Plan
EA Transition Planning
Department of Justice – Office of the CIO

Figure 3-2. IT Strategic Planning Process Summary

Annually in the second quarter of the Fiscal Year, the OCIO PPS staff reviews the IT Strategic Plan to identify any statutory, program or technology changes that warrant a minor update to the plan. Minor updates roughly follow the process described above for the 5-year major plan revisions. However, since minor updates only occur for changes that require an immediate update to the plan, interaction with the major stakeholders occurs only on an as-needed basis.

Following development or update of the IT Strategic Plan, the OCIO will identify the programs and actions for implementing the IT Strategic Plan. OCIO staff offices as well as key Departmental program offices and Components may be identified to lead specific actions to support of one or more of the Programs or Actions identified in the plan. Key performance metrics and indicators are identified for each Program to enable the CIO to track progress toward the IT Strategic Plan goals. These crosscutting priorities are used as input to the EA Transition Planning Process to develop the Target Drivers for each EA segments.

The process diagram in Figure 3-3 shows the sequence of major subprocesses for the IT Strategic Planning Process and the horizontal “swim lanes” identify the stakeholder responsible for each sub-process. The sub-processes are described following the diagram.


IT Strategic Planning Process Diagram
March
April
May
June - July
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
DOJ Oversight
DIRB
DOJ CIO Council
DOJ ITIM Committee
Component Partners
Component CIO
Component Budget/ Finance Staff
Component ITIM Coordinator
Component IT Project Manager
Provide Business Changes, Needs, and Priorities
Conduct Business Leadership Review
Develop Strategies & Prepare Draft IT Strategic Plan
Finalize DOJ IT Strategic Plan
IT Strategic Plan
Conduct DIRB Review
Conduct Component CIO Review

Department of Justice - Office of the CIO

Figure 3-3. IT Strategic Planning Process Diagram

Provide Business Changes, Needs and Priorities. DOJ OCIO will:

- Meet with DOJ Business Leadership to identify program and mission changes, new and evolving statutory requirements and changes in mission priorities that the leadership sees for the Department’s business and mission activities.

Develop Strategies and Prepare Draft IT Strategic Plan. DOJ OCIO will:

- Assess the prior year's accomplishments and evaluate changes in business and mission drivers identified by DOJ business leadership that impact the Department's performance and that require new and innovative IT solutions. Assess current DOJ IT initiatives to see what changes are needed to accommodate the new drivers and what changes in resources, funding and technology are necessary to respond. Assess key technology advances or changes in IT drivers that impact the Plan.
- Prepare a first draft of the IT Strategic Plan that incorporates the business and mission changes, needs and priorities expressed by the DOJ business leadership. Incorporate the DOJ CIO's goals and objectives for the Department's IT resources including security and technology standards, solution and infrastructure consolidations and the key IT directions necessary to enable the business and mission performance objectives.
- Route the draft IT Strategic Plan to the OCIO staffs and Deputy CIOs for review as it is developed and prior to formal review by DOJ Business Leadership and Component CIOs.
- Incorporate appropriate revisions identified during the reviews by OCIO staffs and the Deputy CIOs.

Conduct Business Leadership Review. DOJ OCIO will:

- Meet with DOJ Business Leadership to review the draft IT Strategic Plan and obtain concurrence or recommendations for adjustments to the Plan, if appropriate.

Conduct Component CIO Review. Component CIOs will:

- Review the draft IT Strategic Plan and, through consultation with Component business leaders, concur with or recommend adjustments to the Plan, if appropriate.

Conduct DIRB Review. DOJ OCIO will:

- Brief the Plan to the DIRB and obtain concurrence or recommendations for adjustments to the plan, if appropriate.

Finalize DOJ IT Strategic Plan. The DOJ OCIO will:

- Adjust the draft Plan, as appropriate, from the three reviews.
- Gain final approval from the CIO.
- Secure approval of the Plan by the Deputy Attorney General.
- Distribute the Plan to the Components and publish it on DOJNet.
- Develop a plan of actions and milestones for implementing the key initiatives and programs outlined in the IT Strategic Plan.

Component Self-Governance. The Department's IT Strategic Plan is intended to address all major department-wide and Component needs for IT. Therefore, most Components do not need to create their own IT Strategic Plans.

Component responsibilities in the IT Strategic Planning Process are:

- Component CIOs will review the draft DOJ IT Strategic Plan, identify strategic IT needs that are unique to the Component and ensure those needs are incorporated appropriately into the Department's Plan.
- If a Component IT Strategic Plan is created, provide a copy of the Component plan to the DOJ CIO for review and comment.

3.1.2 EA Transition Planning Process

The EA Transition Planning Process is the second major process of the IT Planning Phase. This process satisfies the requirements for IT architecture planning contained in the OMB EA Assessment Framework and the FEA Practice Guidance.

In the EA Transition Planning Process, the DOJ OCIO creates a mid-term plan to drive current IT investment decisions for the Department. The principal planning activity during the EA Transition Planning Process is the development of the Department Transition Strategy and Sequencing (T&S) Plan. The DOJ EAPMO develops the T&S Plan based on the Department's strategic mission and business goals from the DOJ Strategic Plan, the IT strategic goals and priorities from the DOJ IT Strategic Plan, the actions identified in the ITSP and input from DOJ Components and the OCIO staff.

In the T&S plan, transition strategies, performance objectives and investment priorities are established to guide the Department's IT investment planning. The DOJ EAPMO develops a number of Target Drivers that define the ideal To-Be state for each segment of the Department's Enterprise Architecture. As stated in the Enterprise Performance Management Model (Section 2.5), the T&S plan focuses primarily on the important Department-level IT investments that align with the CIO's priorities from the IT Strategic Plan and the segment architectures developed to implement those priorities. The T&S Plan measures the performance of investments against these Target Drivers to show how the Department is progressing to the To-Be state. These priorities are summarized in IT planning guidance that is developed to aid Components in performing IT investment planning. The summary process diagram below illustrates the high-level tasks within the process, the process outputs and the connection to other processes in the IT governance life cycle.

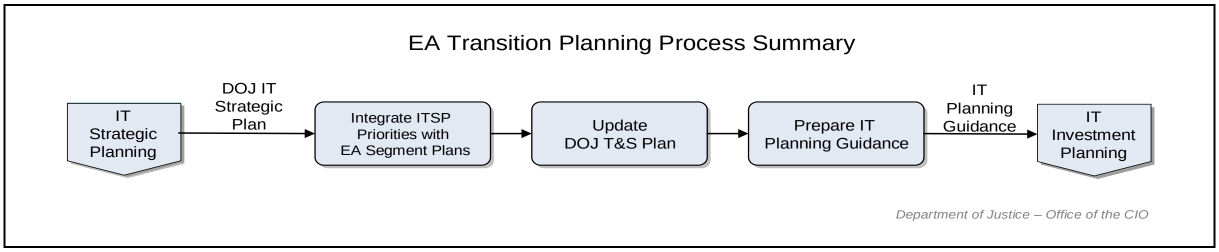

EA Transition Planning Process Summary
IT Strategic Planning
DOJ IT Strategic Plan
Integrate ITSP Priorities with EA Segment Plans
Update DOJ T&S Plan
Prepare IT Planning Guidance
IT Planning Guidance
IT Investment Planning
Department of Justice – Office of the CIO

Figure 3-4. Enterprise Architecture Transition Planning Process Summary

Two products are developed in the EA Transition Planning Process: the DOJ Transition Strategy and Sequencing (T&S) Plan and the IT planning guidance. The T&S Plan describes the EA segment architectures, the business or mission focus of each segment, the strategies for transforming the current architecture to the target enterprise architecture and the key investments that align to each segment in the Department EA.

Target Drivers, based on the priorities from the Department's IT Strategic Plan and the Components' mission needs, are identified in the T&S Plan to help guide near term IT investment planning. The IT planning guidance document summarizes the Department's IT investment priorities and the criteria that will be used to evaluate investment proposals and is provided to Components to aid them in developing Component IT investment plans during the IT Investment Planning Process.

For more information on the EA segment architecture, refer to the DOJ Performance Architecture Document v.3 which is available from the Department OCIO EA PMO.

The process diagram in Figure 3-5 shows the sequence of subprocesses for the EA Transition Planning Process and the swim lanes identify the stakeholder responsible for each sub-process. The sub-processes are described following the diagram.

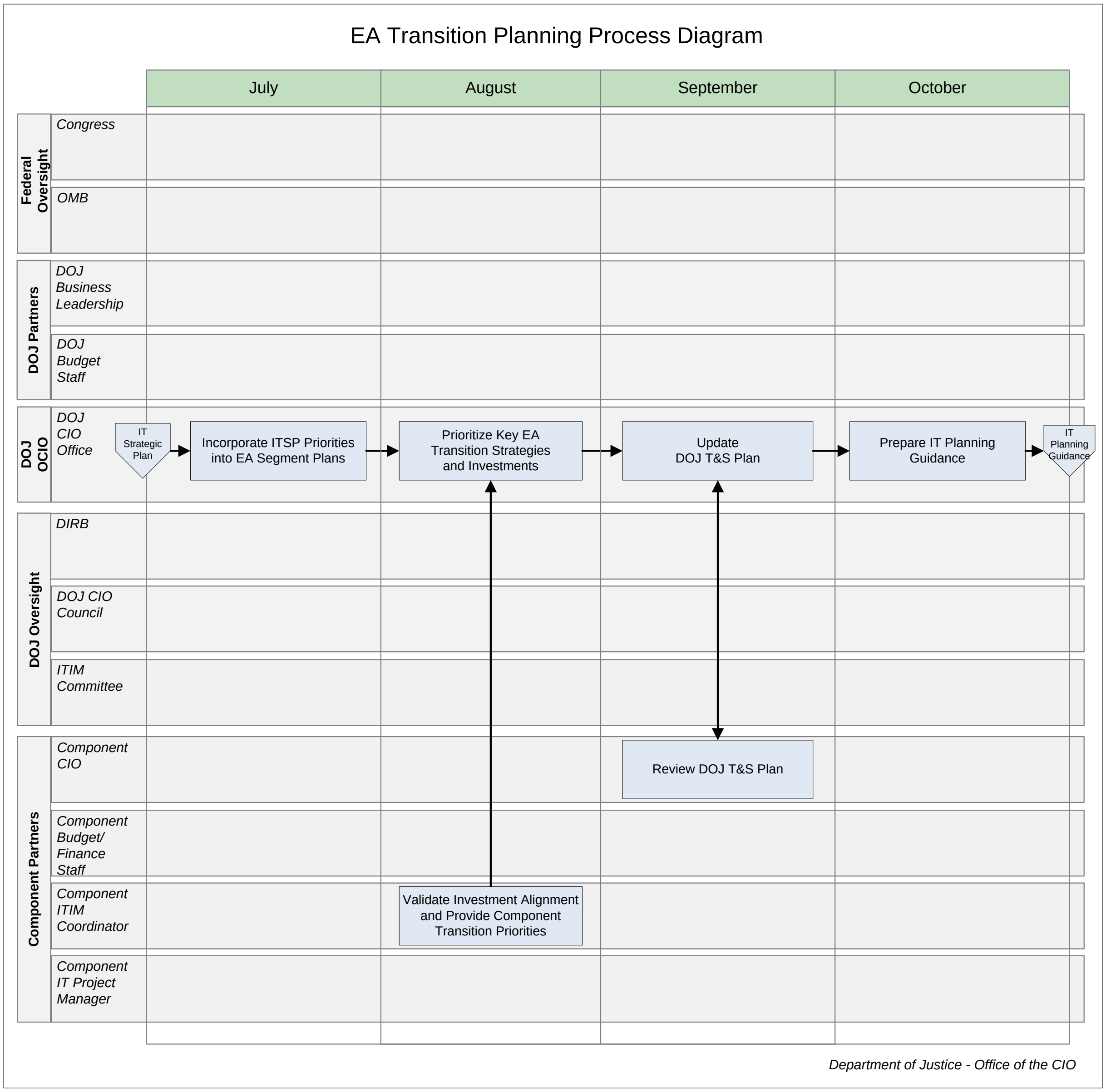

EA Transition Planning Process Diagram
July
August
September
October
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
IT Strategic Plan
Incorporate ITSP Priorities into EA Segment Plans
Prioritize Key EA Transition Strategies and Investments
Update DOJ T&S Plan
Prepare IT Planning Guidance
IT Planning Guidance
DOJ Oversight
DIRB
DOJ CIO Council
ITIM Committee
Component Partners
Component CIO
Review DOJ T&S Plan
Component Budget/ Finance Staff
Component ITIM Coordinator
Validate Investment Alignment and Provide Component Transition Priorities
Component IT Project Manager
Department of Justice - Office of the CIO

Figure 3-5. Enterprise Architecture Transition Planning Process Diagram

Incorporate ITSP Priorities with EA Segment Plans. The DOJ EAPMO will:

- Incorporate the IT priorities described in the IT Strategic Plan and the Department mission priorities into the existing EA segment transition framework through the creation of Target Drivers.
- Integrate the time lines for IT Strategic Plan goals and Department mission goals with the existing Department EA transition time line.

Validate Investment Alignment and Provide Component Transition Priorities. Component ITIM Coordinators will:

- Collaborate with the Component EA point of contact to validate the alignment of Component investments to the Department's segment architectures and provide feedback to DOJ EAPMO.

- Ensure Component transition priorities for mission segment architectures are communicated to the Department EAPMO for incorporation in the Department EA T&S Plan.

Prioritize Key EA Transition Strategies and Investments. The DOJ EAPMO will:
- Prioritize EA transition strategies according to the DOJ IT Strategic Plan priorities.
- Incorporate Component transition priorities for the EA mission segments.
- Review and prioritize the investments in the DOJ IT Portfolio based on the following criteria:
  - Investments that implement key strategic priorities from the IT Strategic Plan or the DOJ Strategic Plan.
  - Investments that align to one of the DOJ EA segments with a detailed architecture and transition plan. For example, the Litigation and Judicial Activities segment.
  - Investments that align with one of the remaining DOJ EA segments and does not propose functionality redundant to an existing investment in the same segment.

Update DOJ T&S Plan. The DOJ EAPMO will:
- Update the milestones and performance metrics for each investment in the DOJ T&S Plan using information reported in the Exhibit 300s, EA data collection activities, as well as from Department oversight reviews of selected investments.
- Update the T&S Plan using the results of the segment analysis, the Component transition priorities and the updated milestone and performance data.
- Incorporate Component comments, if appropriate.
- Present the DOJ T&S Plan to the DOJ CIO for approval.

Review DOJ T&S Plan. The Component CIO will:
- Review the DOJ T&S Plan to ensure Component transition priorities are appropriated prioritized and represented in the plan.

Prepare IT Planning Guidance. The DOJ EAPMO will:
- Summarize the EA transition priorities and investment evaluation criteria into a guidance document that will aid Components in performing IT investment planning.
- Provide the IT planning guidance to Components for use in preparing Component IT Investment Plans for the IT Investment Planning Process.

Component Self-Governance. Component responsibilities in the EA Transition Planning Process are:

- Validate alignment of investments to appropriate EA segments and communicate Component transition priorities for inclusion in the DOJ T&S Plan.
- Review the DOJ T&S Plan to ensure Component investments and transition priorities are accurately represented in the plan.

3.1.3 IT Investment Planning Process.

The IT Investment Planning Process concludes the IT Planning Phase. In this process, the Component CIOs of the largest eight of the Department's Components prepare IT investment plans for the coming budget cycle based on mission and business priorities from their Component business leaders and from the Department's IT planning. The Component CIOs and business leaders collaborate to identify and prioritize IT investments[5] that support Component mission and business priorities and align with the Department's business and mission priorities and IT planning guidance. The DOJ CIO collects the Component IT Investment Plans, reviews the Component plans to identify key investments and meets with Component CIOs to better understand Component IT investment priorities. The DOJ CIO reviews the investment proposals from across the Department and prepares the consolidated DOJ IT Investment Plan as a guide for budget formulation in the Spring IT Budget Planning Process.

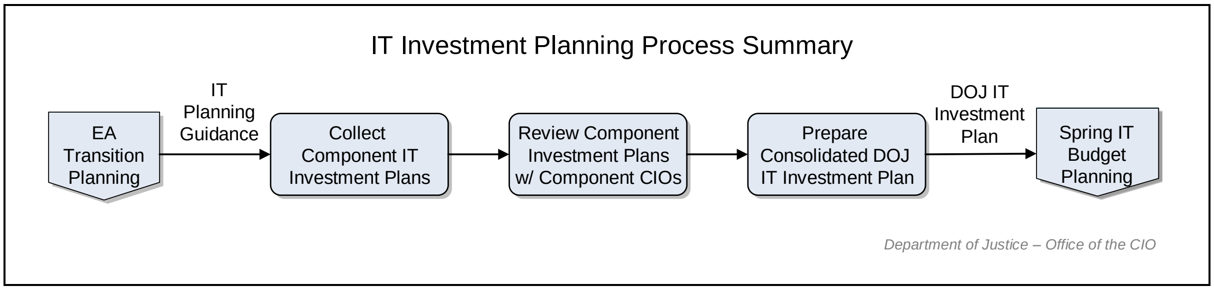

IT Investment Planning Process Summary
EA Transition Planning
IT Planning Guidance
Collect Component IT Investment Plans
Review Component Investment Plans w/ Component CIOs
Prepare Consolidated DOJ IT Investment Plan
DOJ IT Investment Plan
Spring IT Budget Planning
Department of Justice – Office of the CIO

Figure 3-6. IT Investment Planning Process Summary

The DOJ IT Investment Plan identifies the investments with the highest priority for new funding that the DOJ CIO will champion through the Department's budget process. The plan serves as guidance for the Components and the DOJ CIO during the subsequent Spring IT Budget Planning Process.

The following process diagram shows the sequential sub-processing for the IT Investment Planning Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described following the model.

[5] Investments are characterized as being IT based on the definition of IT provided in Section 1.2 and expanded in Appendix B.

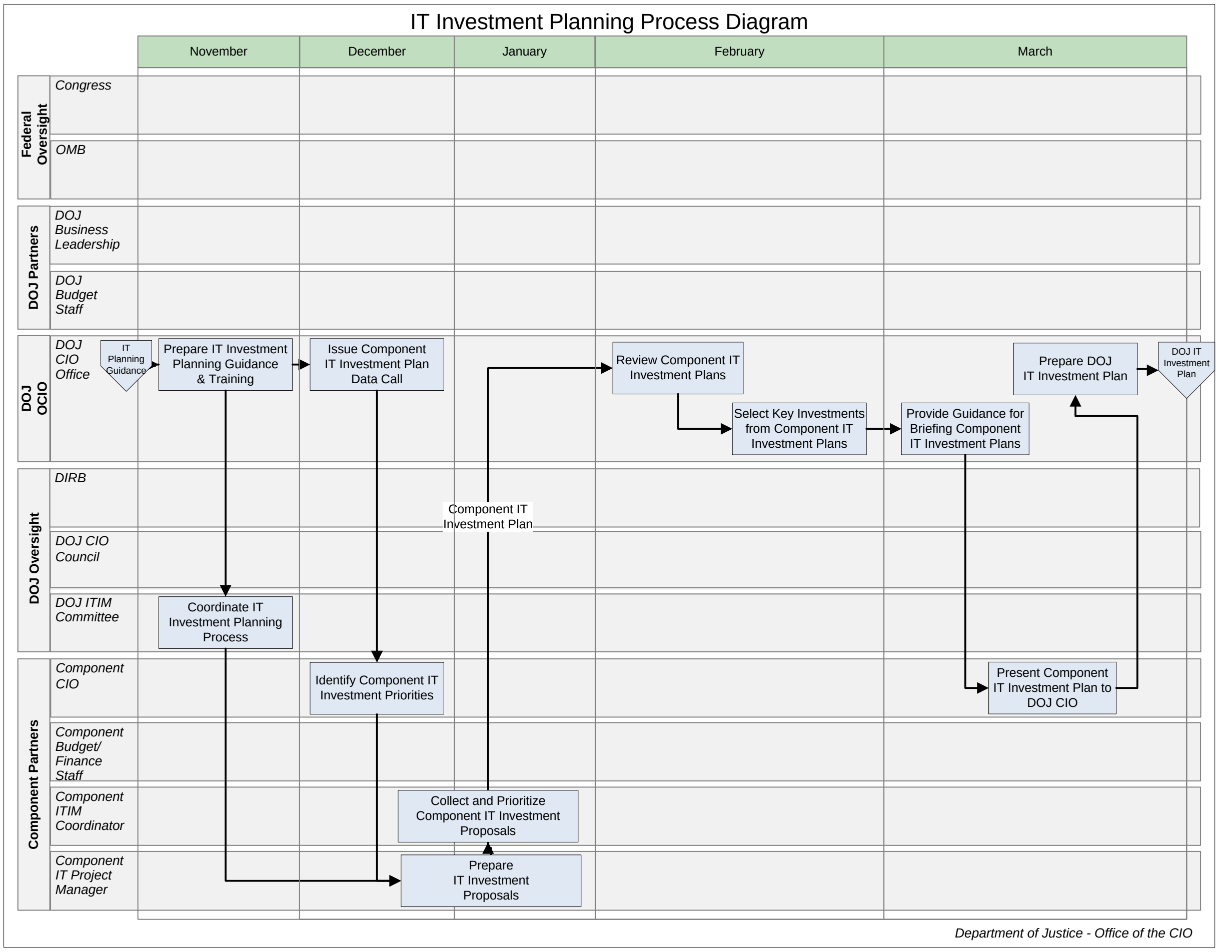

IT Investment Planning Process Diagram
November
December
January
February
March
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
IT Planning Guidance
Prepare IT Investment Planning Guidance & Training
Issue Component IT Investment Plan Data Call
Review Component IT Investment Plans
Select Key Investments from Component IT Investment Plans
Provide Guidance for Briefing Component IT Investment Plans
Prepare DOJ IT Investment Plan
DOJ IT Investment Plan
DOJ Oversight
DIRB
Component IT Investment Plan
DOJ CIO Council
DOJ ITIM Committee
Coordinate IT Investment Planning Process
Component Partners
Component CIO
Identify Component IT Investment Priorities
Present Component IT Investment Plan to DOJ CIO
Component Budget/ Finance Staff
Component ITIM Coordinator
Collect and Prioritize Component IT Investment Proposals
Component IT Project Manager
Prepare IT Investment Proposals
Department of Justice - Office of the CIO

Figure 3-7. IT Investment Planning Process Diagram

Prepare IT Investment Planning Guidance & Training. The DOJ OCIO will:

- Develop IT investment planning instructions that include: the investment planning schedule, IT planning guidance, EA guidance and Department planning priorities.
- Update the Component IT Investment Plan Template (see Appendix D.1) and the instructions for completing the template.
- Develop materials necessary to train the Component ITIM Coordinators who will prepare the Component IT Investment Plans. Schedule the training session.

Issue Component IT Investment Plan Data Call. The DOJ OCIO will:

- Issue the Component IT Investment Plan data call to major IT investor Components. The data call will include the Component IT Investment Plan template, instructions for completing the template and the schedule for submitting the plan to the DOJ CIO.

Coordinate IT Investment Planning Process. The DOJ ITIM Committee will:

- Serve as the forum for coordinating interactions between the major IT investor Components and the DOJ OCIO during the IT Investment Planning Process.

Identify Component IT Investment Priorities. The Component CIO will:

- Work with Component Business Leaders to identify IT investment requirements that support mission and business priorities.
- Prioritize proposed IT investments with Component Business Leaders.

Prepare IT Investment Proposals. The Component IT Project Manager will:

- Develop new investment or enhancement proposals for the upcoming budget cycle.
- Provide the proposals to the Component ITIM Coordinator for review and inclusion in the Component IT Investment Plan.

Collect and Prioritize Component IT Investment Proposals. The Component ITIM Coordinator will:

- Collect IT investment proposals from the Component IT Project Managers.
- Work with the Component EA team to align the investment proposals using the Department IT planning guidance.
- Work with the Component CIO to prioritize the IT investment proposals using the IT planning guidance and internal Component priorities, as appropriate.
- Prepare the Component IT Investment Plan using the ITIP template and submit the draft plan to DOJ OCIO for review.

Review Component IT Investment Plans. The DOJ OCIO will:

- Collect the Component IT Investment Plans.
- Evaluate the IT investment proposals in the Component IT Investment Plans for alignment, performance and compliance using the EA transition guidance, DIRB Summary Reports and results from the Investment Compliance Report as appropriate.
- Recommend to the DOJ CIO key IT investments that should be discussed during the Component IT Investment Plan briefings.

Select Key IT Investments from Component IT Investment Plans. The DOJ CIO will:

- Select the key Component IT investment increase requests and special areas of interest for Component CIOs to discuss during the Component IT Investment Plan briefing.

Provide Guidance for Briefing Component IT Investment Plans. The DOJ OCIO will:

- Develop the Component IT Investment Plan briefing materials including: a proposed schedule, a list of key investments and suggested issues to discuss in the briefing and instructions for completing the briefing template.
- Issue the Component IT Investment Plan briefing guidance to major IT investor Components.

Present Component IT Investment Plan to DOJ CIO. The Component CIO will:

- Develop and present a briefing to the DOJ CIO that highlights the Component's key IT investment increase requests.

Prepare DOJ IT Investment Plan. The DOJ OCIO will:

- Help the DOJ CIO review investment proposals.
- Finalize the DOJ IT Investment Plan.

- Distribute the DOJ IT Investment Plan to Component CIOs and the DOJ Budget Staff for use during the Spring IT Budget Planning Process.

Component Self-Governance. Responsibilities for designated Components during the IT Investment Planning Process are:

- Develop and implement a process for collecting Component IT investment proposals to support mission needs and IT integration objectives.
- Establish a repeatable method for prioritizing IT investment proposals included in the Component IT Investment Plan submitted to the DOJ OCIO.

3.2 IT Budget Phase

The second phase of the governance life cycle is the IT Budget Phase. It begins with the completion of investment planning and concludes when an appropriations act is enacted by Congress and the President.

The IT Budget Phase runs for approximately 18 months, spanning the third and fourth quarters of the Planning Year and the entire period of the Budget Year leading up to enactment and appropriation of funding by the Congress. Because the IT Budget Phase lasts for more than a year, it is important to recognize that the budgets for two succeeding fiscal years are usually under review concurrently, albeit at different stages.

The IT Budget Phase consists of four processes that deliver four key products:

1. The Spring IT Budget Planning Process produces the DOJ Spring IT Budget.

2. The Fall IT Budget Planning Process produces the DOJ Fall IT Budget.

3. The OMB Passback IT Planning Process produces the DOJ Passback IT Budget.

4. The Congressional Budget Planning Process produces the DOJ Enacted IT Budget.

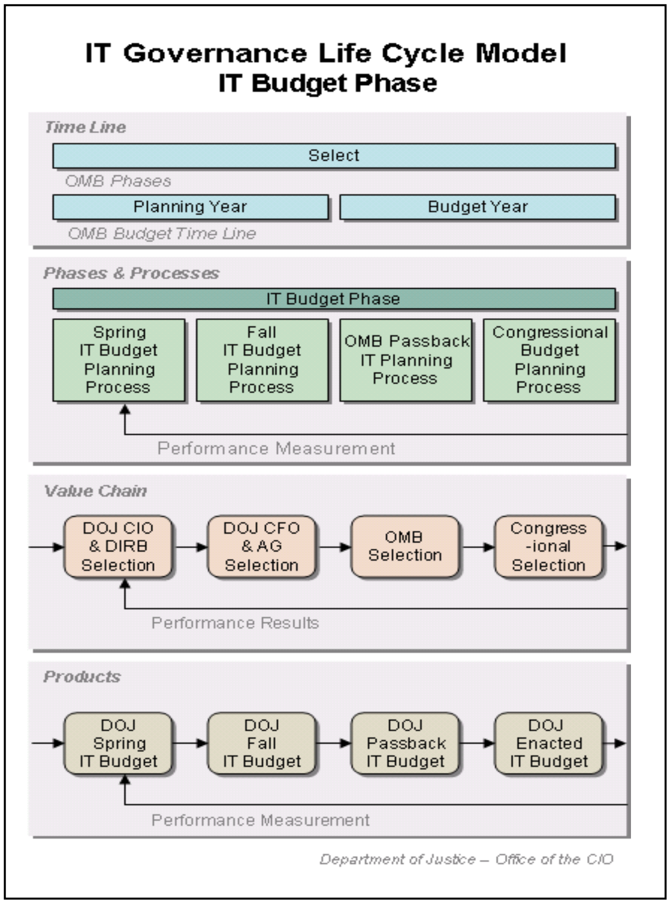


Figure 3-8. IT Governance Investment Life Cycle Model - IT Budget Phase

3.2.1 Spring IT Budget Planning Process

During the Spring IT Budget Planning Process, the Components use internal ITIM selection processes and the DOJ IT Investment Plan to prepare their IT budget requests. The DOJ OCIO collects the Component IT budget requests, evaluates them against the Department IT investment objectives and priorities, prepares the DOJ Spring IT Budget recommendation and submits the budget recommendation for review by the Department IT Investment Review Board (DIRB) and the DOJ Budget Staff.

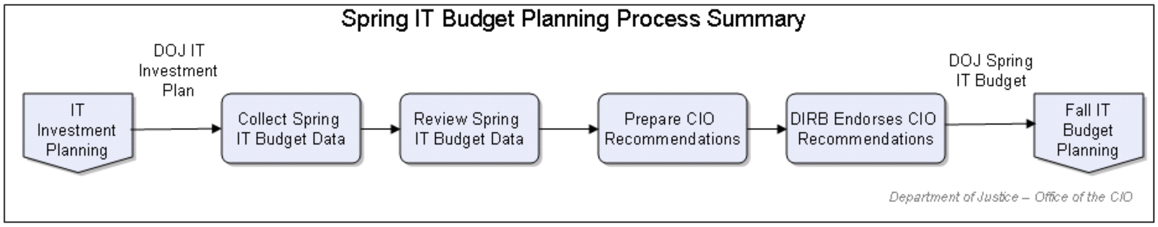

Spring IT Budget Planning Process Summary
DOJ IT Investment Plan
DOJ Spring IT Budget
IT Investment Planning
Collect Spring IT Budget Data
Review Spring IT Budget Data
Prepare CIO Recommendations
DIRB Endorses CIO Recommendations
Fall IT Budget Planning
Department of Justice – Office of the CIO

Figure 3-9. Spring IT Budget Planning Process Summary

The DOJ Spring IT Budget is the DOJ CIO's recommended portfolio of for IT investment for the budget year. It is reviewed by the Department senior leadership during the Fall IT Budget Planning Process as input to final Department budget decisions.

The process diagram in Figure 3-10 shows the sequential sub-processing for the Spring IT Budget Planning Process and the swim lanes show the responsible stakeholder for each sub-process. The sub-processes are described below. Sub-processes shown in light blue in the process diagram are general budget planning steps. Sub-processes shown in light green directly support the preparation of the OMB Exhibit 300.

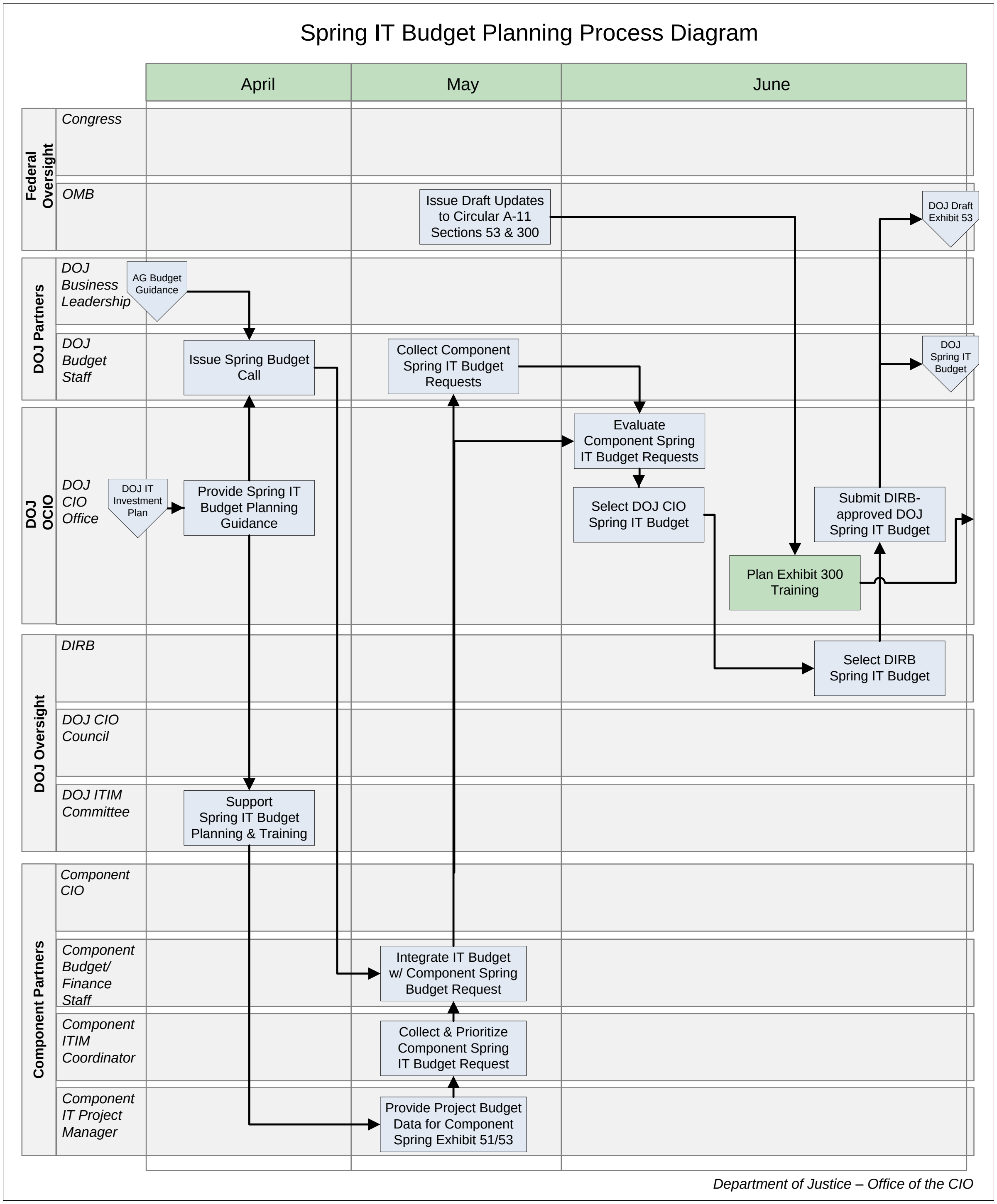

Spring IT Budget Planning Process Diagram
April
May
June
Federal Oversight
Congress
OMB
Issue Draft Updates to Circular A-11 Sections 53 & 300
DOJ Draft Exhibit 53
DOJ Partners
DOJ Business Leadership
AG Budget Guidance
DOJ Budget Staff
Issue Spring Budget Call
Collect Component Spring IT Budget Requests
DOJ Spring IT Budget
DOJ OCIO
DOJ CIO Office
DOJ IT Investment Plan
Provide Spring IT Budget Planning Guidance
Evaluate Component Spring IT Budget Requests
Select DOJ CIO Spring IT Budget
Submit DIRB-approved DOJ Spring IT Budget
Plan Exhibit 300 Training
DOJ Oversight
DIRB
Select DIRB Spring IT Budget
DOJ CIO Council
DOJ ITIM Committee
Support Spring IT Budget Planning & Training
Component Partners
Component CIO
Component Budget/ Finance Staff
Integrate IT Budget w/ Component Spring Budget Request
Component ITIM Coordinator
Collect & Prioritize Component Spring IT Budget Request
Component IT Project Manager
Provide Project Budget Data for Component Spring Exhibit 51/53
Department of Justice – Office of the CIO

Figure 3-10. Spring IT Budget Planning Process Diagram

Prepare Spring IT Budget Planning Guidance and Training. The DOJ OCIO will:

- Prepare Spring IT budget planning guidance to include: the schedule, the investment priorities from the DOJ IT Investment Plan and instructions for completing the Component Exhibit 51/53 (see Appendix D.2).

- Provide the Spring IT budget planning guidance to the DOJ Budget Staff for inclusion in the Department's Spring Budget Call.
- Update or re-issue criteria for identifying investments that require preparation of an Exhibit 300 Capital Asset Plan and Business Case Summary.
- Prepare materials for training the Component ITIM Coordinators to complete the Component Exhibit 51/53 and schedule the training sessions.

Issue Spring Budget Call. The DOJ Budget Staff will:

- Incorporate the Attorney General's budget planning guidance and the OCIO IT budget planning guidance into the Department Spring Budget Call instructions.
- Issue the Spring Budget Call to Components.

Issue Draft Updates to Circular A-11 Sections 53 and 300. OMB will:

- Issue the draft update to OMB Circular A-11 to include: changes to Section 53, OMB Exhibit 53, Section 300 and OMB Exhibit 300.

Support Spring IT Budget Planning and Training. The DOJ ITIM Committee will:

- Support the budget planning process by: reviewing and distributing IT budget planning schedules, providing Component feedback for IT budget exhibits templates and addressing other Component issues during the IT budget planning process.

Provide Project Budget Data for Component Spring Exhibit 51/53. The Component IT Project Manager will:

- Provide project budget data to the Component ITIM Coordinator for inclusion in the Spring Component Exhibit 51/53.

Collect and Prioritize Component Spring IT Budget Request. The Component ITIM Coordinator will:

- Collect project budget data from Component IT Project Managers.
- Work with the Component CIO to prioritize the spring IT budget requests using the DOJ IT Investment Plan as guidance.
- Ensure that the alignment of Component investments to the Department's EA segment architectures is validated with Component EA subject matter experts.
- Work with the Component Budget/Finance staff to prepare the Spring Component Exhibit 51/53 detailing the IT investments in the Component Spring budget request.
- Ensure that all investments that meet the definition of IT (provided in Section 1.2) are included in the Spring Component Exhibit 51/53.

Integrate IT Budget with Component Spring Budget Request. The Component Budget/Finance Staff will:

- Work with the Component ITIM Coordinator to prepare the Spring Component Exhibit 51/53.
- Ensure that all investments that meet the definition of IT (provided in Section 1.2) are included in the Spring Component Exhibit 51/53.
- Submit the Component Spring budget request and Component Exhibit 51/53 to the DOJ Budget Staff and to the DOJ OCIO.

Collect Component Spring IT Budget Requests. The DOJ Budget Staff will:

- Collect Component Spring budget request and Component Exhibit 51/53.
- Forward the Component Spring budget request and Component Exhibit 51/53 to the DOJ OCIO for review and preparation of the DOJ Spring IT Budget.

Evaluate Component Spring IT Budget Requests. The DOJ OCIO Compliance Managers will:

- Review the Component Spring IT budget requests and perform a compliance assessment on each investment requesting new funding.
- Provide a RED, GREEN, or N/A rating for each investment increase requested based on the compliance history of the investment over the past fiscal year.

Select DOJ CIO Spring IT Budget. The DOJ OCIO will:

- Review the Component Exhibit 51/53s for timeliness and completeness.
- Reconcile the Component Exhibit 51/53s with Component budgets.
- Consolidate the Component IT budget requests into a draft CIO's IT budget recommendation working document.
- Evaluate the Component IT budget requests using EA transition guidance and information from Investment Compliance Reports to assign a recommended priority ranking to each request.
- Conduct a preliminary budget review with the DOJ Deputy CIOs and develop proposed investment rankings in preparation for the CIO Spring IT Budget Review.
- Help the DOJ CIO prioritize the Component IT investments in the Spring IT Budget.
- Prepare briefing materials for the DIRB Spring IT Budget Review.

Plan Exhibit 300 Training. The DOJ OCIO will:

- Review the draft updates to OMB Circular A-11 to identify changes to the OMB Exhibit 300 form or the exhibit review process.
- Develop the Exhibit 300 Training Plan.

Select DIRB Spring IT Budget. The DIRB will:

- Review the DOJ CIO Spring IT Budget to ensure that the proposed allocation of funds will meet the Department's IT and business goals, specify necessary changes and ratify the budget for submission to DOJ Budget Staff and review by DOJ executive leadership.

Submit DIRB-approved DOJ Spring IT Budget. The DOJ OCIO will:

- Adjust investment priorities to align with the instructions issued by the DIRB, if required.
- Submit the DOJ Spring IT Budget to the DOJ Budget Staff as the CIO's IT budget recommendation.
- Update eCPIC to reflect the CIO's IT budget recommendation so that the draft Exhibit 53 can be produced.
- Format the DOJ Spring IT Budget into a draft OMB Exhibit 53 and submit the draft OMB Exhibit 53 to OMB for review.

Component Self-Governance. Component responsibilities for the Spring IT Budget Planning Process are:

- Develop and implement a repeatable process for collecting IT budget requests to support mission needs and IT integration objectives.
- Establish a repeatable method for evaluating and prioritizing IT budget requests against internal Component mission priorities and the DOJ IT Investment Plan guidance.
- Work with the Component Budget/Finance Staff to integrate the Spring IT budget request with the Component Spring budget request and to prepare the Component Exhibit 51/53.

3.2.2 Fall IT Budget Planning Process

During the Fall IT Budget Planning Process, the Department's senior leadership selects the IT investments to be included in the Department's Fall budget request to OMB. To accomplish this, the DOJ leadership reviews the DOJ Spring IT Budget recommendation from the DOJ CIO and the Attorney General (AG) selects an approved set of IT investments. The Components then modify their IT budgets to align with the AG's decisions and the DOJ OCIO prepares the DOJ Fall IT Budget for OMB review. The process occurs during the fourth quarter of the fiscal year. During this process, the OMB Exhibit 300s are prepared and reviewed before being submitted to OMB with the DOJ Fall IT Budget.

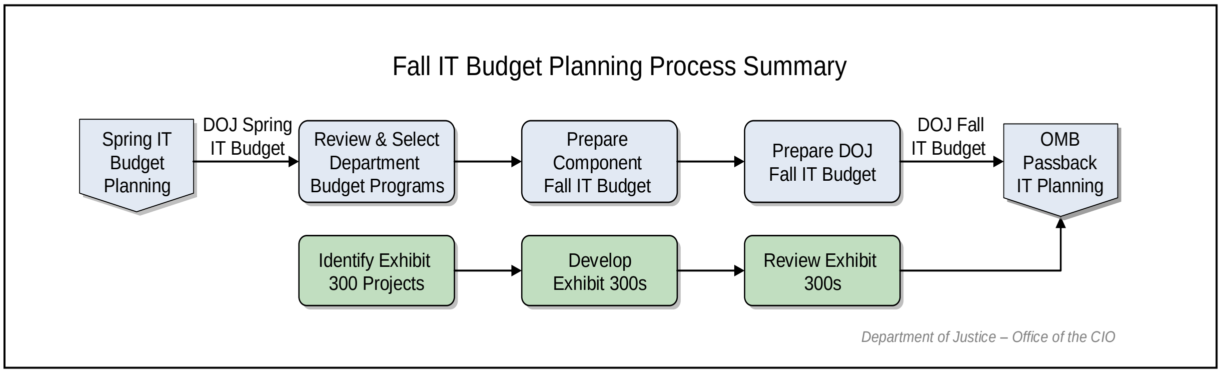

Fall IT Budget Planning Process Summary
Spring IT Budget Planning
DOJ Spring IT Budget
Review & Select Department Budget Programs
Prepare Component Fall IT Budget
Prepare DOJ Fall IT Budget
DOJ Fall IT Budget
OMB Passback IT Planning
Identify Exhibit 300 Projects
Develop Exhibit 300s
Review Exhibit 300s
Department of Justice – Office of the CIO

Figure 3-11. Fall IT Budget Planning Process Summary

The DOJ Fall IT Budget contains the final set of IT investments approved by the Attorney General and consists of the following IT budget exhibits:

OMB Exhibit 53: Agency IT Investment Portfolio Report. This exhibit identifies all of the Department's IT investments[6]. Format and preparation instructions are contained in OMB Circular A-11, Section 53. A sample form is located in Appendix D.3 of this guide.

OMB Exhibit 300: Capital Asset Plan and Business Case Summary. This exhibit

[6] Investments are characterized as being IT based on the definition of IT provided in Section 1.2 and expanded in Appendix B.

documents the project plan and business case for IT investments selected by OMB. The exhibit format and preparation instructions are contained in OMB Circular A-11, Section 300. The current version of OMB Circular A-11 containing a sample Exhibit 300 form can be obtained from the OMB website.

Privacy Impact Assessment (PIA). The PIA documents the risks of exposing personally identifiable information for an investment and describes the actions taken or planned to eliminate or mitigate those risks. The need for a PIA is determined when new systems are being planned for development and each time significant changes for maintaining, collecting and disseminating personally identifiable information (PII) are made to an existing system. The guidelines for preparing the PIA are published by the DOJ Privacy and Civil Liberties Office (PCLO) and the PIA review process is managed by the Privacy Branch within the DOJ OCIO E-Government Services Staff (EGSS).

The process diagram in Figure 3-12 shows the sequential sub-processing for the Fall IT Budget Planning Process and the swim lanes show the responsible stakeholder for each sub-process. The sub-processes are described on the following pages. Sub-processes shown in light blue in the process diagram are general IT budget preparation steps. Sub-processes shown in light green directly support the preparation and review of the OMB Exhibit 300. Sub-processes that are part blue and part green involve both general IT budget preparation and the preparation and review of the Exhibit 300.

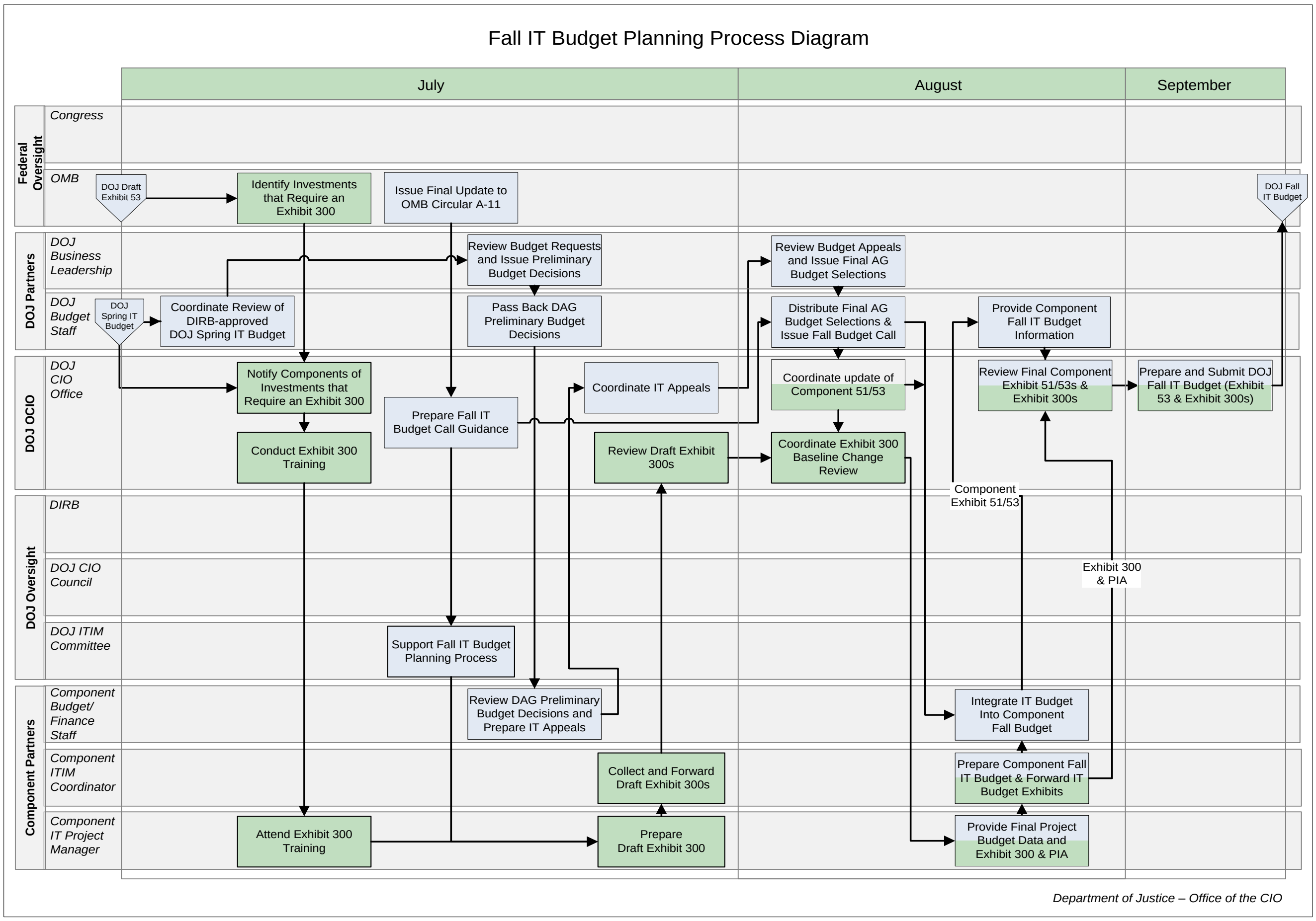

Fall IT Budget Planning Process Diagram
July
August
September
Federal Oversight
Congress
OMB
DOJ Draft Exhibit 53
Identify Investments that Require an Exhibit 300
Issue Final Update to OMB Circular A-11
DOJ Fall IT Budget
DOJ Partners
DOJ Business Leadership
Review Budget Requests and Issue Preliminary Budget Decisions
Review Budget Appeals and Issue Final AG Budget Selections
DOJ Budget Staff
DOJ Spring IT Budget
Coordinate Review of DIRB-approved DOJ Spring IT Budget
Pass Back DAG Preliminary Budget Decisions
Distribute Final AG Budget Selections & Issue Fall Budget Call
Provide Component Fall IT Budget Information
DOJ OCIO
DOJ CIO Office
Notify Components of Investments that Require an Exhibit 300
Coordinate IT Appeals
Coordinate update of Component 51/53
Review Final Component Exhibit 51/53s & Exhibit 300s
Prepare and Submit DOJ Fall IT Budget (Exhibit 53 & Exhibit 300s)
Prepare Fall IT Budget Call Guidance
Conduct Exhibit 300 Training
Review Draft Exhibit 300s
Coordinate Exhibit 300 Baseline Change Review
Component Exhibit 51/53
DOJ Oversight
DIRB
DOJ CIO Council
Exhibit 300 & PIA
DOJ ITIM Committee
Support Fall IT Budget Planning Process
Component Partners
Component Budget/ Finance Staff
Review DAG Preliminary Budget Decisions and Prepare IT Appeals
Integrate IT Budget Into Component Fall Budget
Component ITIM Coordinator
Collect and Forward Draft Exhibit 300s
Prepare Component Fall IT Budget & Forward IT Budget Exhibits
Component IT Project Manager
Attend Exhibit 300 Training
Prepare Draft Exhibit 300
Provide Final Project Budget Data and Exhibit 300 & PIA
Department of Justice – Office of the CIO

Figure 3-12. Fall IT Budget Planning Process Diagram

Coordinate Review of DIRB-approved DOJ Spring IT Budget. The DOJ Budget Staff will:

- Review the DIRB-approved DOJ Spring IT Budget for alignment with DOJ budget priorities and provide budget recommendations for consideration by senior leadership.
- Coordinate the review of the Spring IT Budget by the Department's senior leadership team for selection of the Fall Department budget.

Identify Investments that Require an Exhibit 300. OMB will:

- Review DOJ's draft OMB Exhibit 53 and select IT investments that require an OMB Exhibit 300.
- Inform the DOJ CIO of the investments selected.

Notify Components of Investments that Require an Exhibit 300. The DOJ OCIO will:

- Notify Components of the investments that will require an OMB Exhibit 300.

Conduct Exhibit 300 Training. The DOJ OCIO will:

- Train the Component IT Project Managers to prepare the OMB Exhibit 300.

Attend Exhibit 300 Training. The Component IT Project Manager will:

- Attend the Exhibit 300 training provided by the DOJ OCIO.

Issue Final Update to OMB Circular A-11. OMB will:

- Issue the final version of OMB Circular A-11 for the Fall budget submission, including the final OMB Exhibit 53 and OMB Exhibit 300 forms and submission instructions.

Prepare Fall IT Budget Call Guidance. The DOJ OCIO will:

- Review the final updates to OMB Circular A-11.
- Prepare Fall IT budget call instructions including: the schedule, templates and instructions for preparing the Component Exhibit 51/53, OMB Exhibit 300 and PIA.
- Provide the IT budget call schedule to DOJ Budget Staff for inclusion in the Department's Fall Budget Call.
- Brief the ITIM Committee on the Fall IT budget call schedule and budget preparation instructions.

Support Fall IT Budget Planning Process. The DOJ ITIM Committee will:

- Support the Fall IT Budget Planning Process by distributing IT budget planning information and serving as the forum for resolving Component IT budget planning issues.

Review Budget Requests and Issue Preliminary Budget Decisions. The DOJ Business Leadership will:

- Review the Spring IT budget request along with Spring budget requests from Components and make preliminary budget selections for the Department's Fall budget.
- Provide the preliminary budget decisions to the DOJ Budget Staff for review and

appeal.

Pass Back DAG Preliminary Budget Decisions. The DOJ Budget Staff will:

- Distribute the results of the DAG preliminary budget review to Components and provide instructions for the submission and review of budget appeals.

Review DAG Preliminary Budget Decisions and Prepare IT Appeals. The Component Budget/Finance Staffs will:

- Coordinate review of the DAG preliminary budget decisions.
- Work with the Component CIO to identify any impacts to critical IT investments.
- Prepare and submit appeals, when appropriate, according to the appeal instructions.

Coordinate IT Appeals. The DOJ OCIO will:

- Coordinate the preparation of appeals for critical IT investments for the AG's final budget review.

Prepare Draft Exhibit 300. The Component IT Project Manager will:

- Prepare the draft OMB Exhibit 300 for investments selected by OMB.
- Forward the draft OMB Exhibit 300 to the Component ITIM Coordinator for internal Component review and approval. Revise as needed.

Collect and Forward Draft Exhibit 300s. The Component ITIM Coordinator will:

- Collect the draft OMB Exhibit 300s from Component IT Project Managers.
- Coordinate internal review of the OMB Exhibit 300s for accuracy and completeness.
- Ensure that the draft Exhibit 300s are entered into the DOJ CIO's Electronic Capital Planning and Investment Control (eCPIC) investment management tool.
- Notify the DOJ OCIO when the draft Component Exhibit 300s have been entered into eCPIC and are ready for review and comment.

Review Draft Exhibit 300s. The DOJ OCIO will:

- Review the draft OMB Exhibit 300s using the review criteria provided in Appendix D.6 and identify weaknesses.
- Inform the Components of weaknesses discovered and recommended corrective actions.

Review Budget Appeals and Issue Final AG Budget Selections. The DOJ Business Leadership will:

- Review budget appeals submitted by Components for consideration by the AG.
- Issue final AG budget selections for the Fall Budget Call.

Distribute Final AG Budget Selections and Issue Fall Budget Call. The DOJ Budget Staff will:

- Distribute the final AG budget selections to the Components.
- Issue the Fall Budget Call including the schedule for submitting IT budget exhibits.

Coordinate update of Component 51/53. The DOJ OCIO will:

- Provide Components with instructions for the review of Component 51/53s with AG's

Final budget Selection changes.

Coordinate Exhibit 300 Baseline Change Review. The DOJ OCIO will:

- Provide Components with instructions for the review of Exhibit 300s with proposed project baseline changes.

Provide Final Project Budget Data and Exhibit 300 & PIA. The Component IT Project Manager will:

- Update the investment budget data and align it with the AG's budget decisions.
- Provide final investment budget data to the Component ITIM Coordinator for inclusion in the Fall Component Exhibit 51/53.
- Update and align the IT investment budget data and project plan in the OMB Exhibit 300 with the data submitted for the Component Exhibit 51/53.
- Forward the final OMB Exhibit 300 and PIA to the Component ITIM Coordinator.

Prepare Component Fall IT Budget & Forward IT Budget Exhibits. The Component ITIM Coordinator will:

- Incorporate project budget updates into the Component IT budget request.
- Work with the Component Budget/Finance Staff to align the Component IT budget with the AG final budget decisions and prepare the Fall Component Exhibit 51/53.
- Collect final OMB Exhibit 300s and PIAs from the Component IT Project Managers.
- Ensure the final OMB Exhibit 300 data and OMB Exhibit 53 data is entered into the DOJ CIO's eCPIC investment management tool and notify the DOJ OCIO when Exhibit 300s are ready for review and submission to OMB.
- Forward new or updated PIAs to DOJ OCIO for review.

Integrate IT Budget into Component Fall Budget. The Component Budget/Finance Staff will:

- Work with the Component ITIM Coordinator to align the Component IT budget with the AG final budget decisions and prepare the Fall Component Exhibit 51/53.
- Submit the Component Fall budget and Exhibit 51/53 to the DOJ Budget Staff and DOJ OCIO.

Provide Component Fall IT Budget Information. The DOJ Budget Staff will:

- Collect the Component Fall budgets from the Component Budget/Finance Staffs.
- Forward the Fall Component Exhibit 51/53s to DOJ OCIO to support review of the Component Fall IT budget and preparation of the DOJ Fall IT Budget.

Review Final Component Exhibit 51/53s & 300s. The DOJ OCIO will:

- Collect final Fall Component Exhibit 51/53s from the DOJ Budget Staff.
- Reconcile Component Exhibit 51/53s with Component Fall budgets and identify any discrepancies.
- Review the final OMB Exhibit 300s and PIAs from Components.
- Evaluate the Component budget exhibits for timeliness and completeness.
- Notify Component ITIM Coordinators when corrective action is needed.
- Prepares a Component Exhibit 51 for each Component budget account from the Component Exhibit 51/53s and sends the Component Exhibit 51 to DOJ Budget Staff.

Prepare and Submit DOJ Fall IT Budget (Exhibit 53 & 300s). The DOJ OCIO will:

- Prepare the IT Capital Plan as specified by OMB Circular A-130.
- Prepare the final DOJ OMB Exhibit 53 for submission to OMB.
- Submit the IT Capital Plan, OMB Exhibit 53, OMB Exhibit 300s and PIAs to OMB in the format prescribed in OMB Circular A-11.

Component Self-Governance. Component responsibilities for the Fall IT Budget Planning Process are:

- Review Department budget decisions, identify items for appeal, if necessary and prepare IT budget appeal justifications.
- Implement a repeatable process for collecting and reviewing Exhibit 300s for major IT investment projects, as required.
- Work with the Component Budget/Finance Staff to align the Component Exhibit 51/53 with AG final budget decisions.

3.2.3 OMB Passback IT Planning Process

During the OMB Passback IT Planning Process, the Department's Fall IT Budget request is reviewed by OMB for incorporation into the President's Budget. This process occurs during the first quarter of the fiscal year. Three primary activities occur during this process. OMB reviews the DOJ Fall IT Budget and provides a "passback" package to the Department detailing OMB's review decisions. The Department updates the IT program budgets to align with OMB's decisions and prepares the Passback IT Budget for OMB to incorporate into the President's Budget. Concurrently, OMB reviews the Exhibit 300s and the Department updates and prepares the Passback Exhibit 300s for OMB to submit to Congress with the President's Budget.

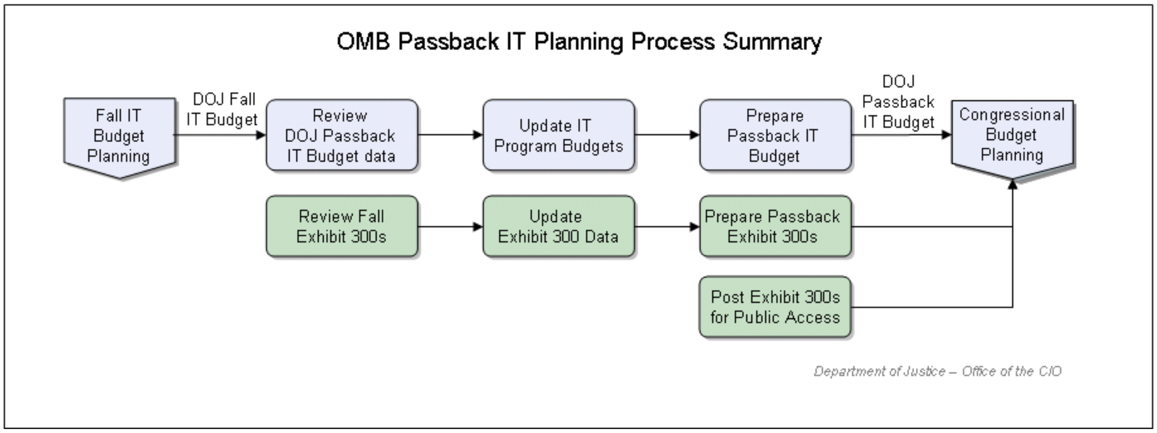
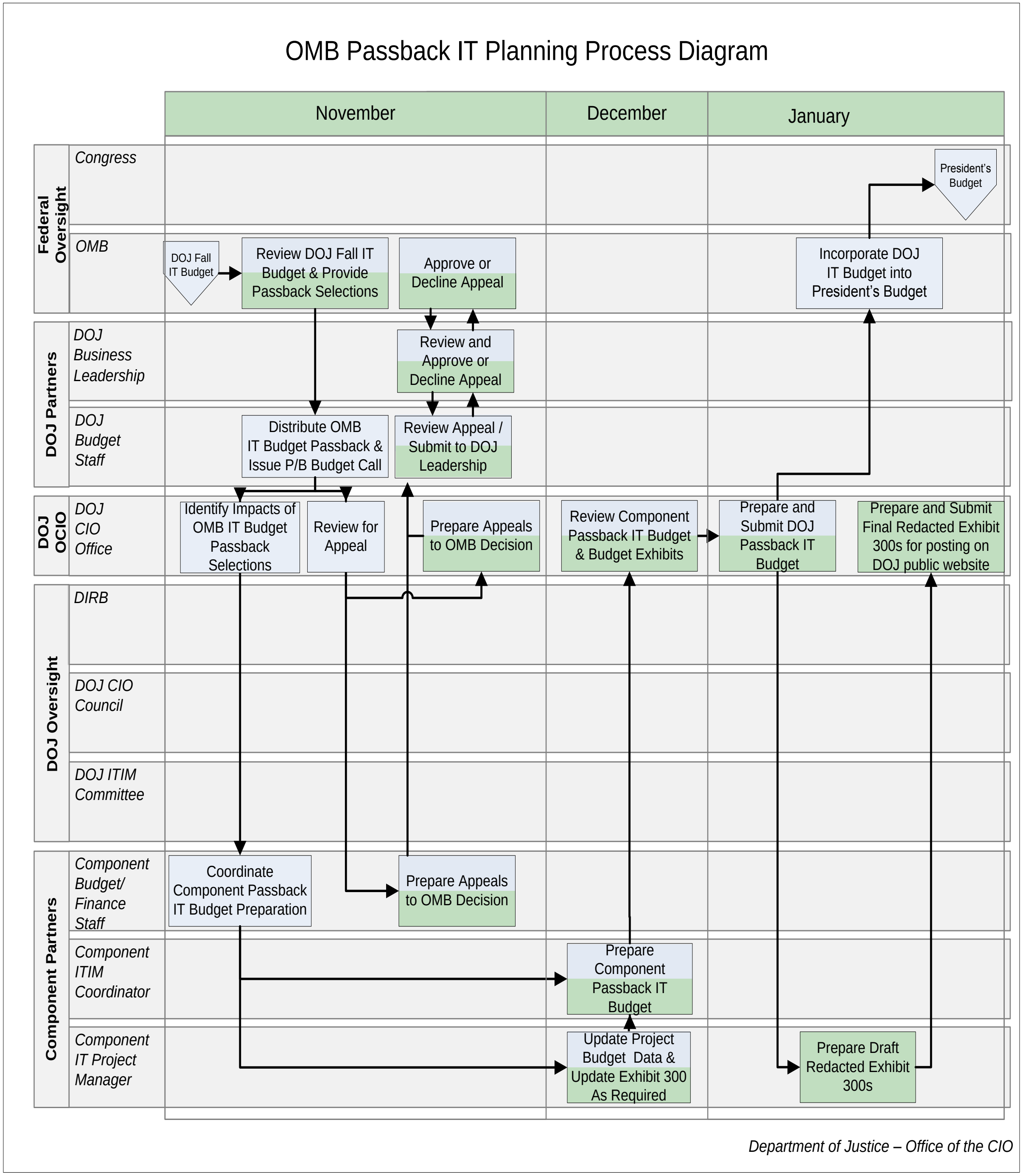

OMB Passback IT Planning Process Summary
Fall IT Budget Planning
DOJ Fall IT Budget
Review DOJ Passback IT Budget data
Update IT Program Budgets
Prepare Passback IT Budget
DOJ Passback IT Budget
Congressional Budget Planning
Review Fall Exhibit 300s
Update Exhibit 300 Data
Prepare Passback Exhibit 300s
Post Exhibit 300s for Public Access
Department of Justice – Office of the CIO

Figure 3-13. OMB Passback IT Planning Process Summary

The DOJ Passback IT Budget contains the final budget request agreed upon by OMB and the Department. OMB incorporates the Passback IT Budget into the President's Budget submitted to Congress for review and enactment of budget legislation.

The process diagram in Figure 3-14 shows the sequential sub-processing for the Congressional Budget Planning Process and the swim lanes show the responsible stakeholder for each sub-process. The sub-processes are described on the pages following the diagram. Sub-processes shown in light blue in the process diagram are general budget planning steps. Sub-processes shown in light green directly support the preparation and review of the OMB Exhibit 300. Sub-processes that are part blue and part green involve general budget preparation and preparation and review of the Exhibit 300.


OMB Passback IT Planning Process Diagram
November
December
January
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
DOJ Oversight
DIRB
DOJ CIO Council
DOJ ITIM Committee
Component Partners
Component Budget/ Finance Staff
Component ITIM Coordinator
Component IT Project Manager
President's Budget
DOJ Fall IT Budget
Review DOJ Fall IT Budget & Provide Passback Selections
Approve or Decline Appeal
Incorporate DOJ IT Budget into President's Budget
Review and Approve or Decline Appeal
Distribute OMB IT Budget Passback & Issue P/B Budget Call
Review Appeal / Submit to DOJ Leadership
Identify Impacts of OMB IT Budget Passback Selections
Review for Appeal
Prepare Appeals to OMB Decision
Review Component Passback IT Budget & Budget Exhibits
Prepare and Submit DOJ Passback IT Budget
Prepare and Submit Final Redacted Exhibit 300s for posting on DOJ public website
Coordinate Component Passback IT Budget Preparation
Prepare Appeals to OMB Decision
Prepare Component Passback IT Budget
Update Project Budget Data & Update Exhibit 300 As Required
Prepare Draft Redacted Exhibit 300s

Department of Justice – Office of the CIO

Figure 3-14. OMB Passback IT Planning Process Diagram

Review DOJ Fall IT Budget & Provide Passback Selections. OMB will:

- Review the DOJ IT Budget as part of the Department budget review.
- Provide budget passback selections to the DOJ Budget Staff.
- Review DOJ OMB Exhibit 300s and provide results to the DOJ OCIO.

Distribute OMB IT Budget Passback & Issue P/B Budget Call. The DOJ Budget Staff will:

- Review the OMB Passback and distribute IT budget passback decisions to DOJ CIO.
- Coordinate presentation of budget appeals to OMB and communicate appeal decisions to the Components concerned.
- Provide instructions to Components for submitting OMB passback budget revisions.

Identify Impacts of OMB IT Budget Passback Selections. The DOJ OCIO will:

- Review the OMB IT budget passback to identify the impacts to IT projects.
- Prepare the Passback Executive Summary and provide the summary to the DOJ CIO.
- Work with DOJ Budget Staff and Component OCIOs to submit IT program appeals and to adjust IT budgets, when necessary.
- Coordinate passback action times from OMB for the CIO.

Review for Appeal. The DOJ OCIO will:

- Review the OMB IT budget passback to identify any items that should be appealed.

Prepare Appeal to OMB Decision. The DOJ OCIO / Component Budget Staff will:

- Prepare any necessary appeals and send them to the DOJ Budget Staff.

Review Appeal / Submit to DOJ Leadership. The DOJ Budget Staff will:

- Review any appeals it receives.
- Prepare the Appeal to DOJ Leadership decision.
- Prepare Approved appeals for OMB decision.
- Send Approved appeals to OMB.

Review Appeal and Approve or Decline Appeal. The DOJ Leadership will:

- Review any appeals it receives.
- Approve or Decline an appeal.
- Send all appeals back to the DOJ Budget Staff.

Approve or Decline Appeal. The OMB will:

- Review any appeals it receives.
- Approve or Decline an appeal.
- Send all appeals back to the DOJ Budget Staff.

Coordinate Component Passback IT Budget Preparation. The Component Budget/Finance Staff will:

- Distribute OMB passback decisions affecting Component IT investments and coordinate update of the Component IT budget.

Update Project Budget Data & Update Exhibit 300 As Required. The Component IT Project Manager will:

- Update project budget data to reflect OMB passback decisions.
- Update the OMB Exhibit 300 with prior year actual data and budget changes, as required.
- Provide the updated project budget data and updated OMB Exhibit 300 to the Component ITIM Coordinator to update the Component IT budget.

Prepare Component Passback IT Budget. The Component ITIM Coordinator will:

- Collect updated project budget data from the Component IT Project Managers.
- Work with the Component Budget/Finance Staff to prepare the Passback Component Exhibit 51/53.
- Collect updated OMB Exhibit 300s from Component IT Project Managers and forward the updated OMB Exhibit 300s to the DOJ OCIO for review and submission to OMB.
- Update eCPIC to reflect the OMB's Passback Budget for both Exhibit 300 and Exhibit 51/53 investments.

Review Component Passback IT Budget & Budget Exhibits. The DOJ OCIO will:

- Collect the updated Component Exhibit 51/53 and OMB Exhibit 300s from Components and evaluate the exhibits for timeliness and completeness.
- Reconcile the Component Exhibit 51/53s with budget information from the DOJ Budget Staff and work with the Component ITIM Coordinators to resolve any discrepancies.

Prepare and Submit DOJ Passback IT Budget. The DOJ CIO Office will:

- Prepare the final updated OMB Exhibit 300s for submission to OMB.
- Update the OMB Exhibit 53 for submission to OMB.
- Submit the updated OMB Exhibit 53 and the OMB Exhibit 300s to OMB as instructed.

Prepare Draft Redacted Exhibit 300s. The Component IT Project Managers will:

- Coordinate with Component ITIM Coordinators to prepare draft redacted Exhibit 300s in accordance with the DOJ OCIO instructions for redacting Exhibit 300s (see http://10.173.2.12/jmd/irm/pps/itim/itim_policyguidance.php)
- Coordinate with Component CIO and Business Leadership to ensure the redacted Exhibit 300s do not contain sensitive information.

Prepare and Submit Final Redacted Exhibit 300s for posting to the DOJ public website. The DOJ CIO Office will:

- Review and prepare the final redacted Exhibit 300s for posting to the DOJ public website.
- Submit the final redacted Exhibit 300s to DOJ Budget Staff and the OCIO e-Gov staff for posting.

Incorporate DOJ IT Budget into President's Budget. OMB will:

- Incorporate the DOJ Passback IT Budget into the President's Budget.
- Submit the President's Budget to Congress for review.

Component Self-Governance. Component responsibilities for the OMB Passback IT Planning Process are:

- Define and implement a repeatable process for reviewing OMB passback decisions for impact to IT budget requests and selecting IT budget appeals, if necessary.
- Work with the Component Budget/Finance Staff to align the Component Exhibit 51/53 with OMB budget decisions.
- Review the accuracy of prior year cost data for all investments, update as needed and provide CIO verification of the information.

3.2.4 Congressional Budget Planning Process

The purpose of the Congressional Budget Planning Process is for the Congress to review the President's Budget request and enact budget legislation to fund Federal government operations for the coming fiscal year. This process occurs from February to September of each year. The process begins when OMB submits the President's Budget to Congress for review. Congress reviews the agency budget proposals in the President's Budget and after deliberation and debate, drafts and enacts legislation to fund the DOJ Enacted IT Budget for the coming fiscal year. As part of this process, all OMB Exhibit 300s must be made available for public access and review.

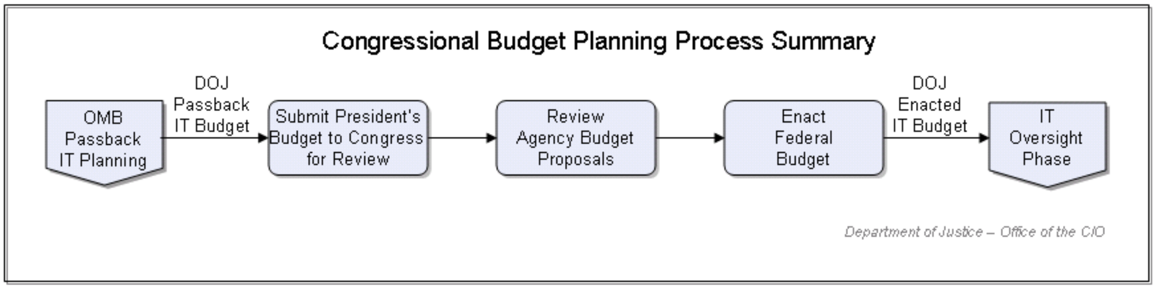

Congressional Budget Planning Process Summary
OMB Passback IT Planning
DOJ Passback IT Budget
Submit President's Budget to Congress for Review
Review Agency Budget Proposals
Enact Federal Budget
DOJ Enacted IT Budget
IT Oversight Phase
Department of Justice – Office of the CIO

Figure 3-15. Congressional Budget Planning Process Summary

The DOJ Enacted IT Budget specifies the funding authorized for IT investments for the current fiscal year. The DOJ CIO and Components are responsible for managing the funds appropriated to achieve desired program outcomes. These outcomes are reviewed and assessed during the IT Oversight Phase.

The process diagram in Figure 3-16 shows the sequential sub-processing for the Congressional Budget Planning Process and the swim lanes identify the stakeholder responsible for each sub-process. The sub-processes are described on the pages following the diagram. Sub-processes shown in light blue on the process diagram are general IT budget planning steps. Sub-processes shown in light green directly support preparation and posting of the OMB Exhibit 300 Capital Asset Plan and Business Case.

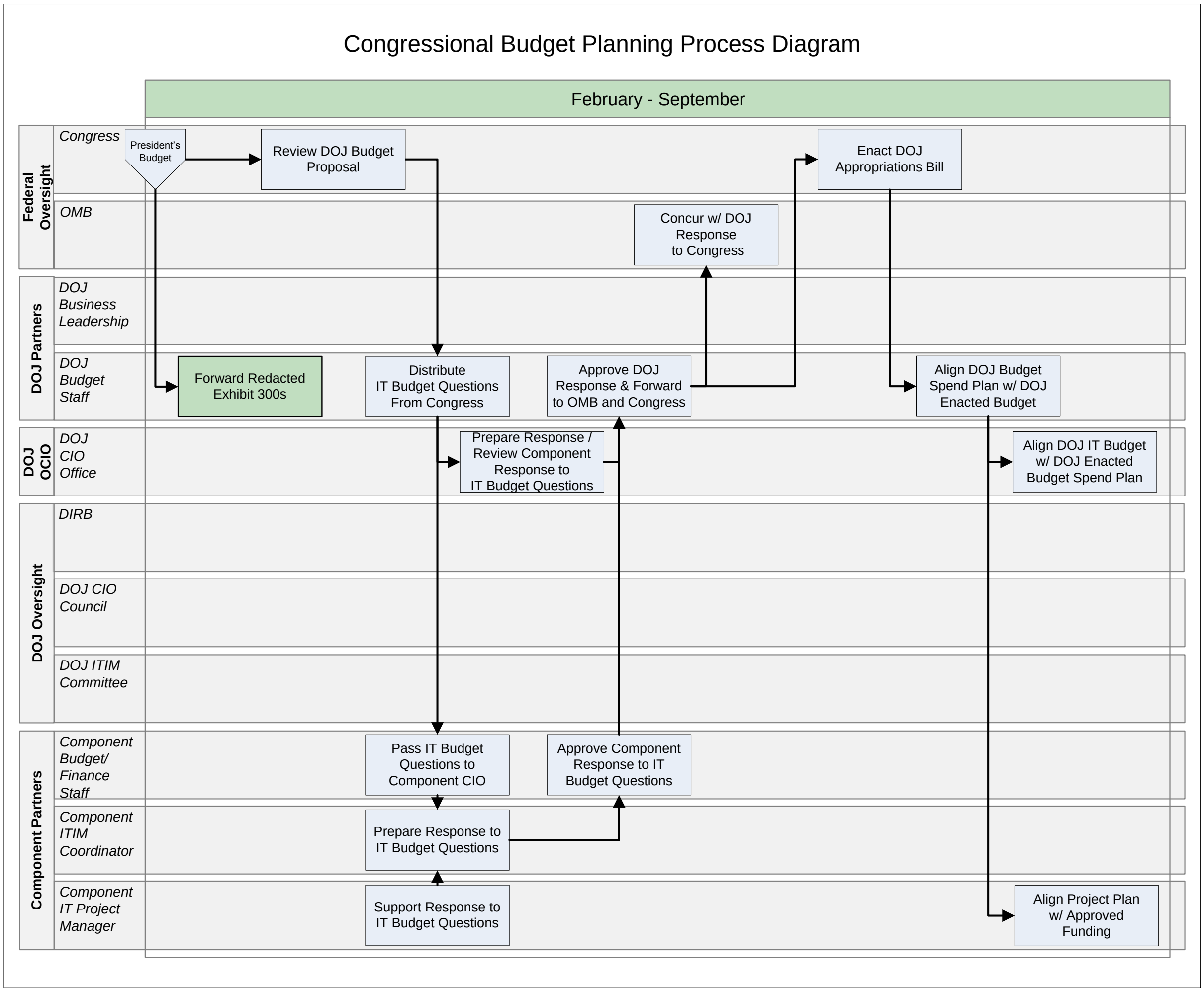

Congressional Budget Planning Process Diagram
February - September
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
DOJ Oversight
DIRB
DOJ CIO Council
DOJ ITIM Committee
Component Partners
Component Budget/ Finance Staff
Component ITIM Coordinator
Component IT Project Manager
President's Budget
Review DOJ Budget Proposal
Enact DOJ Appropriations Bill
Concur w/ DOJ Response to Congress
Forward Redacted Exhibit 300s
Distribute IT Budget Questions From Congress
Approve DOJ Response & Forward to OMB and Congress
Align DOJ Budget Spend Plan w/ DOJ Enacted Budget
Prepare Response / Review Component Response to IT Budget Questions
Align DOJ IT Budget w/ DOJ Enacted Budget Spend Plan
Pass IT Budget Questions to Component CIO
Approve Component Response to IT Budget Questions
Prepare Response to IT Budget Questions
Support Response to IT Budget Questions
Align Project Plan w/ Approved Funding

Figure 3-16. Congressional Budget Planning Process Diagram

Post Redacted Exhibit 300s. The DOJ Budget Staff will:

- Post the redacted OMB Exhibit 300s to the Department's public web site.

During the course of Congressional committee budget hearings and deliberations, the following actions occur:

Review DOJ Budget Proposal. The Congressional committees will:

- Review the Department's budget proposal in the President's Budget.
- Evaluate the programs and IT investments requested and prepare draft budget legislation.
- Submit Questions for the Record (QFRs) to the Department regarding funds for IT investments requested in the budget.
- Conduct budget hearings and draft budget recommendations for legislative action.

Distribute IT Budget Questions from Congress. The DOJ Budget Staff will:

- Distribute IT budget QFRs received from Congressional committees for response by the DOJ OCIO or the Component Budget/Finance Staffs.

Prepare Response / Review Component Response to IT Budget Questions. The DOJ OCIO will:

- Prepare responses to Congressional QFRs for DOJ CIO managed investments and/or review Component responses to IT budget questions as needed.

Pass IT Budget Questions to Component CIO. The Component Budget/Finance Staff will:

- Pass QFRs regarding Component IT investments to the Component CIO for preparation of a response.

Prepare Response to IT Budget Questions. The Component OCIO will:

- Work with the Component Budget/Finance Staff and DOJ CIO if necessary, to prepare a timely response to Congressional QFRs.

Support Response to IT Budget Questions. The Component IT Project Manager will:

- Provide information necessary to prepare responses to QFRs.

Approve and Forward Component Response to IT Budget Questions. The Component Budget/Finance Staff will:

- Review the proposed response prepared by the Component OCIO and forward the proposed response to DOJ Budget Staff for review and forwarding to Congress.

Approve DOJ Response and Forward to OMB and Congress. The DOJ Budget Staff will:

- Review the proposed response submitted by the Component and route it to the DOJ CIO for review and comment, when appropriate.
- Forward the proposed response to OMB for review and concurrence.
- Forward the final response to OMB and Congress.

Concur with DOJ Response to Congress. OMB will:

- Review the Department's proposed response to Congress, recommend changes, when necessary and concur with the final response.

After Congressional committees have drafted the final appropriations bill, the Congress will take action to enact legislation authorizing the Department's budget. The major activities are:

Enact DOJ Appropriations Bill. Congress will:

- Negotiate the final appropriations bill and enact legislation to fund DOJ operations for the coming fiscal year.

Align Budget Spend Plan w/ DOJ Enacted Budget. The DOJ Budget Staff will:

- Align the Budget Spend Plan with the DOJ Budget enacted into law.

Align DOJ IT Budget w/ DOJ Enacted Budget Spend Plan. The DOJ OCIO will:

- Work with Components to align the DOJ IT Budget with the DOJ Enacted Budget Spend Plan.

Align Project Plan w/ Approved Funding. The Component IT Project Manager will:

- Align the project plan with the funds allotted from the DOJ Enacted IT Budget.
- Execute the project plan to achieve the funded project objectives.

Component Self-Governance. Component responsibilities during the Congressional Budget Planning Process are:

- Provide IT investment information as needed to support the Congressional budget review process.
- Review and update IT project plans and OMB Exhibit 300s, as necessary, to execute the Enacted IT Budget.

3.3 IT Oversight Phase

The IT Oversight Phase is the third and longest duration phase of the IT governance life cycle. IT investments are funded in the previous phase and monitored for satisfactory progress and results in the IT Oversight Phase. This phase is continuously ongoing, monitoring investments through their life cycle, beginning with planning and development, continuing through implementation and operations and maintenance (O&M) and concluding with retirement.

Figure 3-17 shows how the IT Oversight Phase relates to the OMB Phases and GAO Budget Timeline and shows the two processes and the products associated with the phase.

1. The Executive Review Process generates DIRB Meeting Summaries, DIRB Action Reports and Program Certification report.

2. The Compliance Review Process generates OMB reports, the consolidated Compliance Report, as well as individual investment oversight reports.

The IT Oversight Model discussion in Section 2.7 describes the Department's oversight structure, including key oversight stakeholders, the types of review processes and products and the interactions between oversight processes and other governance processes. The following sections describe the processing activities of the Executive Review Process and Compliance Review Process.

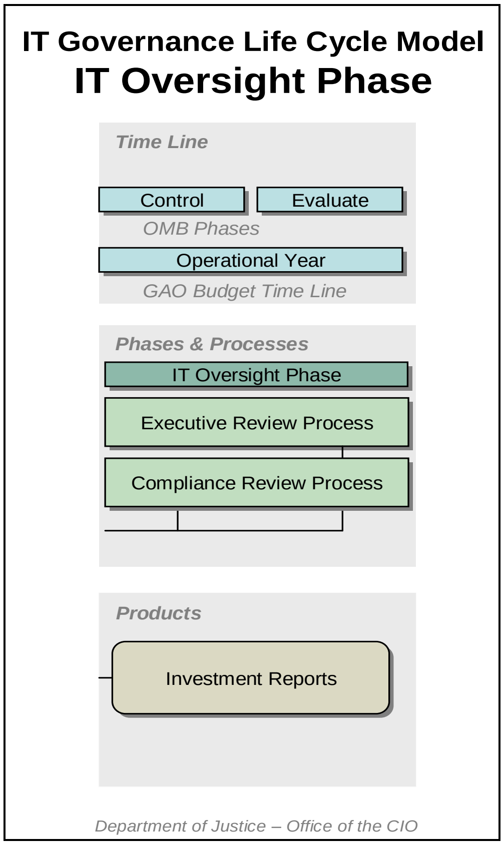
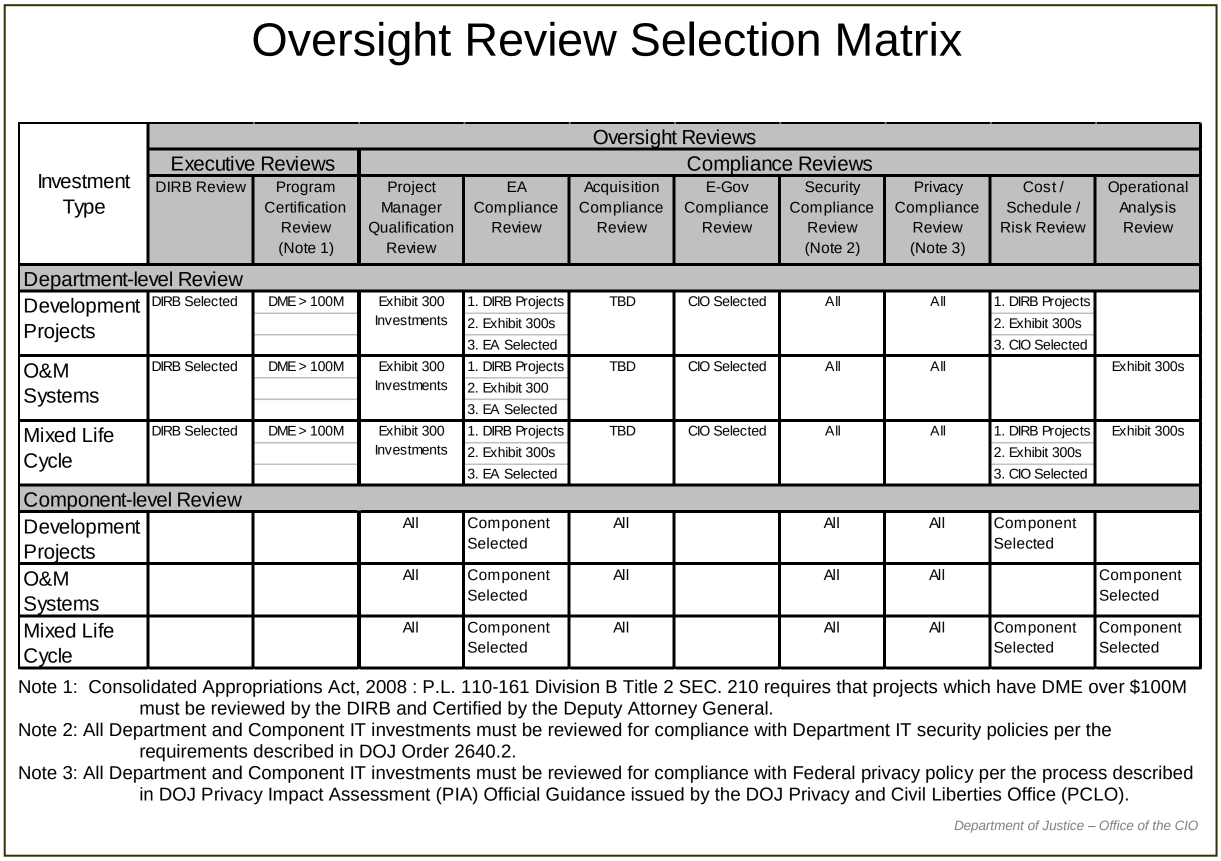


Figure 3-17. IT Governance Life Cycle - IT Oversight Phase

The Oversight Review Selection Matrix on the next page provides a guide for determining the oversight reviews required for each investment type. The model identifies the ten different types of oversight reviews across the top and the three Operational State classifications defined in the Investment Classification Model in Section 2.6. The Oversight Review Selection Matrix is divided to show that reviews occur at the Department level and at the Component level. The criteria for selecting investments for each type of review is listed in the grid block below each review type. The selection criteria for Department-level reviews are listed briefly in the model and are defined in more detail in the compliance review descriptions on the following pages. The selection criteria for Component-level reviews must be defined by Components unless there is Department-wide policy that specifies the criteria to be used (e.g., Notes 1, 2 and 3).



Oversight Review Selection Matrix

Investment Type	Oversight Reviews									
	Executive Reviews		Compliance Reviews							
	DIRB Review	Program Certification Review (Note 1)	Project Manager Qualification Review	EA Compliance Review	Acquisition Compliance Review	E-Gov Compliance Review	Security Compliance Review (Note 2)	Privacy Compliance Review (Note 3)	Cost / Schedule / Risk Review	Operational Analysis Review
Department-level Review										
Development Projects	DIRB Selected	DME > 100M	Exhibit 300 Investments	1. DIRB Projects 2. Exhibit 300s 3. EA Selected	TBD	CIO Selected	All	All	1. DIRB Projects 2. Exhibit 300s 3. CIO Selected	
O&M Systems	DIRB Selected	DME > 100M	Exhibit 300 Investments	1. DIRB Projects 2. Exhibit 300 3. EA Selected	TBD	CIO Selected	All	All		Exhibit 300s
Mixed Life Cycle	DIRB Selected	DME > 100M	Exhibit 300 Investments	1. DIRB Projects 2. Exhibit 300s 3. EA Selected	TBD	CIO Selected	All	All	1. DIRB Projects 2. Exhibit 300s 3. CIO Selected	Exhibit 300s
Component-level Review										
Development Projects			All	Component Selected	All		All	All	Component Selected	
O&M Systems			All	Component Selected	All		All	All		Component Selected
Mixed Life Cycle			All	Component Selected	All		All	All	Component Selected	Component Selected

Note 1: Consolidated Appropriations Act, 2008 : P.L. 110-161 Division B Title 2 SEC. 210 requires that projects which have DME over $100M must be reviewed by the DIRB and Certified by the Deputy Attorney General.

Note 2: All Department and Component IT investments must be reviewed for compliance with Department IT security policies per the requirements described in DOJ Order 2640.2.

Note 3: All Department and Component IT investments must be reviewed for compliance with Federal privacy policy per the process described in DOJ Privacy Impact Assessment (PIA) Official Guidance issued by the DOJ Privacy and Civil Liberties Office (PCLO).

Department of Justice – Office of the CIO

Figure 3-18. Oversight Review Selection Matrix.

3.3.1 Executive Review Process

The Department Executive Review Process applies to a select set of important investments that require executive level oversight because of their high cost, high risk, or high visibility or require specific review to comply with legislative requirements.[7] Investments selected for executive review are typically multi-year development projects that impact or require integration with other important Department systems, programs, Components, or other executive agencies. The Department IT Investment Review Board (DIRB) performs the executive review for the Department's IT program.

The DIRB is chartered to oversee the management of the Department's IT investments and to ensure that these investments are aligned with the Department's mission and goals. The DIRB is chaired by the Deputy Attorney General (DAG); the other members include: the Department Chief Information Officer (CIO), the Department Chief Financial Officer (CFO) and four other senior executives. The board accomplishes its purpose in two ways: first, by reviewing the Department's IT investment portfolio during the Department's budget review

[7] Consolidated Appropriations Act, 2008 : P.L. 110-161 Division B Title 2 SEC. 210 requires the DIRB to review and the DAG to certify that projects having total development costs over $100M have "appropriate program management and contractor oversight mechanisms in place and that the program is compatible with the enterprise architecture".

process (discussed in the IT Budget Phase) and second, by conducting periodic reviews of selected Department-level high profile, high cost, or high risk IT investments to ensure that appropriate business value and acceptable return on investment (ROI) are being delivered. In short, the DIRB ensures that the Department invests in the "Right Thing," and that IT investments are managed in the "Right Way" to achieve the "Right Result."

Because the Executive Review Process requires a high degree of coordination between project management offices (PMOs) and the board, the DIRB charter established an Executive Secretariat to coordinate the scheduling of review meetings, assist PMOs in preparing for reviews and to manage the various administrative functions of coordinating and publishing the DIRB schedule, preparing and posting reports, tracking completion of action items and distributing project information to board members. The DIRB Executive Secretariat supports the DOJ CIO on all matters concerning the DIRB and acts as the principal liaison between the board and the PMOs of projects being reviewed by the DIRB.

Process Summary. Each Fall, the DOJ CIO and the DIRB chair review the Department's IT portfolio, select a set of critical investment projects to be reviewed by the DIRB during the coming fiscal year and establish the tentative project review schedule. Throughout the fiscal year, the DIRB appraises the progress of the selected investments to ensure they are proceeding according to plan and are still sound investments for the Department and continue to provide relevance to the Components and the Department's goals. Typically, the DIRB reviews two projects each month. After each project review, the board votes to determine whether the members believe the project is on track and is being properly managed. The board may direct the Project Manager or other stakeholders to complete specific corrective actions, provide reports, or prepare specific SDLC documentation to remedy deficiencies identified during the review. Based on the outcome of the board's vote, projects may be required to report to the board each quarter, or less frequently depending on the board's assessment. The results of each review are compiled into reports that document project status and monitor progress for subsequent reviews. The information in the reports is also used to support investment and budget planning decisions during the IT Budget Phase. The Executive Review Process Summary below provides an overview of the process, its outputs and the connection to the IT Budget Phase.

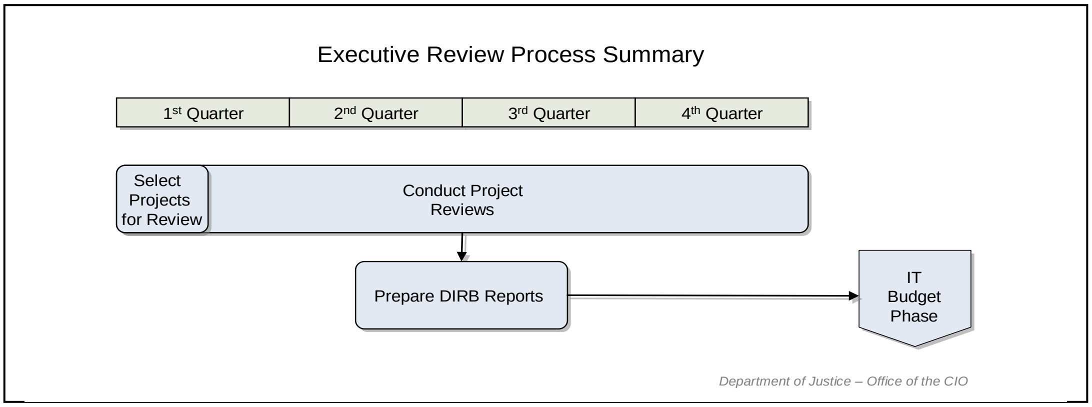


Figure 3-19. IT Governance - Executive Review Process

The DIRB reports produced from the Executive Review Process serve the following purposes:

- Document meeting proceedings, identify key project issues discussed and record action items assigned during the DIRB review.[8]
- Report the DIRB's recommendation for program certification according to requirements specified by Congress.
- Record the current status, progress and completion of action items assigned by the DIRB. Examples of DIRB reports are shown in Appendix E.

The following process diagram shows the sequential subprocessing for the Executive Review Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the following pages.

Note: At the time this version of the IT Governance Guide was being developed, the Program Certification process was still being finalized. As such, the next version of the Guide will incorporated the appropriate changes to the Executive Review Process.

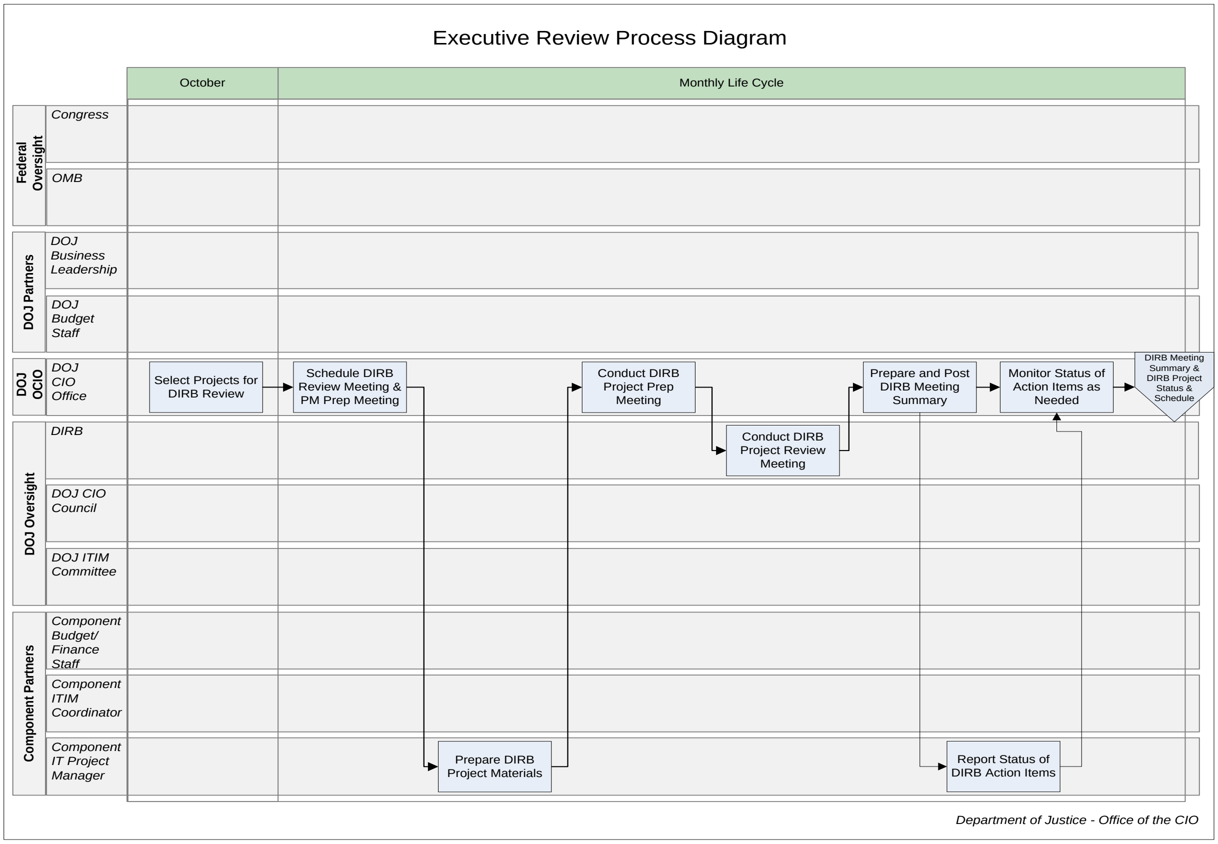

Executive Review Process Diagram
October
Monthly Life Cycle
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
DOJ Oversight
DIRB
DOJ CIO Council
DOJ ITIM Committee
Component Partners
Component Budget/ Finance Staff
Component ITIM Coordinator
Component IT Project Manager
Select Projects for DIRB Review
Schedule DIRB Review Meeting & PM Prep Meeting
Prepare DIRB Project Materials
Conduct DIRB Project Prep Meeting
Conduct DIRB Project Review Meeting
Prepare and Post DIRB Meeting Summary
Report Status of DIRB Action Items
Monitor Status of Action Items as Needed
DIRB Meeting Summary & DIRB Project Status & Schedule
Department of Justice - Office of the CIO

Figure 3-20. Executive Review Process Diagram

[8] Because the DIRB project review often includes business sensitive and predecisional financial information, the project review briefing and DIRB Meeting Summary are categorized and handled as "controlled unclassified information", previously called "sensitive but unclassified" information. If classified information is addressed before the DIRB, appropriate additional access and information handling procedures are implemented.

Select Projects for DIRB Review. At the beginning of each fiscal year, the CIO consults with the DAG to select 10-15 investments for DIRB project review over the course of the fiscal year. The selected projects, commonly referred to as "DIRB Projects," are chosen based on at least one of the following criteria:

- **High Profile:** A high profile project is one that has high interest beyond the project office either inside or outside the department. For example, a high profile project may receive extensive media coverage or Congressional interest.
- **High Cost**: A high cost project is any project that requires an Exhibit 300 be completed.
- **High Risk**: A high risk project is a large project involving multiple politically sensitive issues with significant cost and schedule variance that would drastically affect the entire project in addition to business objectives that are unlikely to be achieved.
- **DAG or CIO Discretion:** Projects may be added or removed at any time during the fiscal year at the discretion of the DAG or CIO.
- **Select Projects for Certification Review.** Identify projects that require special review according to requirements specified by Congress.[9]

Schedule Executive Review Meeting and PM Prep Meeting. The DOJ OCIO will:

- Prepare and manage the DIRB Project List throughout the year, adding new projects when necessary and removing projects that no longer require executive review.
- Prepare and maintain the DIRB Schedule and Status Report throughout the course of the year.
- Monthly, notify the DOJ OCIO front office of the Executive Reviews planned for the coming month and supply a list of mandatory and optional attendees for each review.
- Schedule the specific date, time and location of the Executive Review Meetings.
- Contact the appropriate Component CIO and IT Project Manager to inform them of the date and time the review will be held and provide the Component IT Project Manager with the DIRB Review Template (see Appendix D.3).
- Schedule a review preparation meeting with the Component IT Project Manager 1-2 weeks prior to the Executive Review meeting.

Prepare Project Briefing Materials. The Component IT Project Manager will:

- Prepare the DIRB presentation by filling out the DIRB Review Template and organize any relevant follow-up materials relating to the last DIRB session.
- Submit an electronic draft copy of the DIRB Review Template and relevant follow up materials to the DIRB Exec. Sec. at least two business days before the review.

Conduct DIRB Project Prep Meeting. The DOJ OCIO (DIRB Exec. Sec.) will:

- Meet with Component IT Project Manager in advance of DIRB to review the presentation and follow up on any action items if necessary. The purpose of this meeting is to confirm that all necessary information is included in the briefing, which, once it has been finalized, is referred to as the "DIRB Deck."
- Distribute an electronic copy of the briefing and last Meeting Summary to all DIRB members at least one business day before the Executive Review is scheduled to occur.

[9] Consolidated Appropriations Act, 2008 : P.L. 110-161 Division B Title 2 SEC. 210

Conduct Executive Review Meeting. The DIRB will:

- Conduct a meeting to evaluate the project. During the first part of the review, the Component IT Project Manager will present the DIRB Deck and answer questions from the board members. After the presentation is over, the Component IT Project Manager will be excused from the room and the DIRB will discuss the project.
- Vote to rate the project as Green, Yellow or Red in two categories: Project Issues[10] and Project Management. [11]
- Assign action items, when necessary. These items state what actions the Component IT Project Manager must complete before the next DIRB in order to address issues identified during the review. Action items may include preparation of specific SDLC documentation.

Prepare and Post DIRB Meeting Summary. The DOJ OCIO (DIRB Exec. Sec.) will:

- Document the meeting's proceedings in a DIRB Meeting Summary. The Summary will include a list of all attendees, the final DIRB vote and a list of action items to be completed before the next Executive Review. It will outline highlights of the discussion between the DIRB and Component IT Project Manager and among DIRB members (See Appendix D.4).
- Submit the Summary to the DOJ CIO front office for edits and CIO approval.
- Update the DIRB records based on the information reported at the DIRB review.
- Send the Summary to the Component IT Project Manager for review and comment after the DOJ CIO has approved it.
- Make any necessary changes and post the final version of the Summary in the DIRB directory on the JCON G Drive.
- Send an electronic copy of the Summary to all DIRB members.

Report the Status of DIRB Action Items. The Component IT Project Manager will:

- Report the completion of action items assigned by the DIRB, provide appropriate deliverables and provide a status report of progress for uncompleted action items. These reports will be provided on a monthly basis to the OCIO DIRB Executive Secretariat or as specified by the DIRB.

Monitor the Status of Action Items as Needed. The DOJ OCIO (DIRB Exec. Sec.) will:

- Work with CIO staff to complete any assigned action items assigned to OCIO before the next DIRB review.
- Contact the Component IT Project Manager to determine status of actions items assigned to the PMO and obtain appropriate documentation of action item status.

[10] **DIRB Voting Options for Project Issues:**

Green	Investment has no major issues	DIRB review in one year (or major milestone)
Yellow	Significant issues, but manageable	DIRB review in six months
Red	Major issues, requires corrective action	DIRB review within three months

[11] **DIRB Voting Options for Project Management:**

Green	Full confidence in the PMO	**No corrective actions**
Yellow	Qualified confidence in the PMO	**Possible action items**
Red	Lack of confidence in the PMO	**Chair will meet with Executive Sponsor**

- Document the completion of action items in the DIRB action item records. Inform the DIRB members when actions are closed and distribute documentation that closes action items, when appropriate.

Component Self-Governance. Component responsibilities for the Executive Review Process are:

- Elevate projects with significant governance, budget and/or performance issues to the DOJ CIO for consideration for DIRB review, as appropriate.
- Develop an internal monitoring process for projects selected for DIRB review.
- Implement a similar process for reviewing important Component IT projects.

3.3.2 Compliance Review Process

The Compliance Review Process is used to determine how well investments are being managed to comply with Department and Federal IT policies and standards. All active Projects and O&M investments are subject to some aspect of the Compliance Review Process. The Compliance Managers responsible for each compliance area schedule and conduct reviews throughout the fiscal year to satisfy the specific reporting requirement associated with the review. Compliance Review information is used to prepare the Compliance Report for the IT Budget Phase.

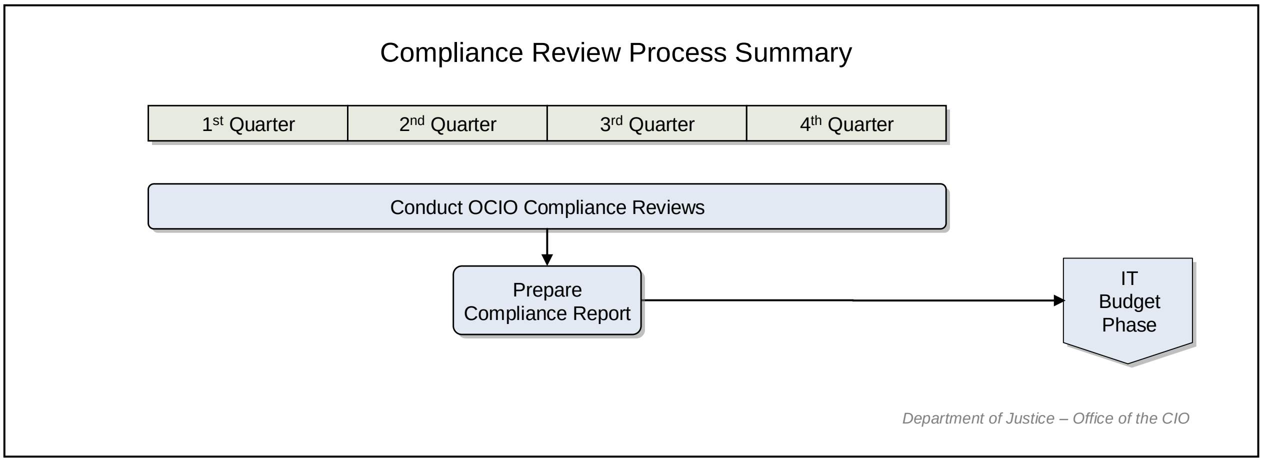

Compliance Review Process Summary
1st Quarter
2nd Quarter
3rd Quarter
4th Quarter
Conduct OCIO Compliance Reviews
Prepare Compliance Report
IT Budget Phase
Department of Justice – Office of the CIO

Figure 3-21. Compliance Review Process Summary

The Compliance Review Process consists of two main activities – conducting one or more of the eight individual compliance reviews and preparing the Compliance Report. The Compliance Report provides feedback to senior executives and planners about investment compliance performance to support IT investment and budget decision-making during the IT Budget Phase.

Compliance Reviews. The Department-level compliance reviews conducted by the DOJ OCIO operate as independent, but complementary, processes under the management of an assigned OCIO staff. The results of these reviews are used to assign ratings of Green

(Satisfactory) or Red (Unsatisfactory) on the Compliance Report prepared during the IT Budget Phase. As described in the IT Oversight Model in Section 2.7, oversight of IT investments is performed at two levels – the Department and the Component. In most cases, a relatively small number of key investments are selected for review at the Department level based on very specific selection criteria. Investments not reviewed at the Department-level are considered Component-level investments.

The descriptions of the Department compliance reviews on the following pages include: the DOJ OCIO process owner, the review purpose, the timing or frequency for each review, a brief description of the review process including a process diagram and a description of the reports that are produced from the review.

Compliance Reviews

Project Management Qualification (PMQ) Review. Reviews the qualifications of project managers for compliance with the Federal IT Project Manager Guidance from the Federal CIO Council.

Enterprise Architecture (EA) Review. Reviews alignment of investments to segment architectures to prevent duplication and to identify opportunities for consolidation or standardization of technologies or services.

Acquisition (ACQ) Review. Reviews software and support service procurements for compliance with government-wide acquisition regulations and use of Federal or Department-wide software license and support service blanket purchase agreements.

E-Government (E-Gov) Review. Reviews investments identified as part of the Department's E-Government Implementation Plan for completion of OMB-approved milestones.

Security (Sec) Review. Reviews all systems and applications for compliance with Federal and Department IT security policies and specifications.

Privacy (PIA) Review. Monitors the preparation, approval and posting of Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) for compliance with OMB and DOJ privacy policies.

Cost/Schedule/Risk (C/S/R) Review. Reviews development projects to ensure acceptable progress toward on-budget and on-time delivery and effective management of project risks.

Operational Analysis (OA) Review. Reviews selected high cost O&M investments to ensure they continue to effectively deliver their operational goal(s) and meet approved cost targets.

3.3.2.1 IT Project Manager Qualification Review

The Project Management Qualification (PMQ) Review is conducted by the Enterprise Solutions Staff Compliance Manager to comply with the requirements of OMB memorandum M-04-19 entitled "Information Technology Project Manager Qualification Guidance" and DOJ Information Resources Management Policy DOJ Order 2880.1B. The Department and its Components use the criteria contained in the Federal IT Project Manager Guidance Matrix issued by the Federal CIO Council to determine if IT project managers for all IT investments possess the necessary project management competencies and suggested work experience appropriate to the investments they are assigned to manage. The review performed by the DOJ OCIO is designed to ensure that IT project managers for important Department-level projects are qualified according to the criteria in the Federal CIO Council Federal IT Project Manager Guidance Matrix. The review is performed annually during the review of Exhibit 300 business cases for the Fall IT Budget Planning Process described in section 3.2.2. The results of the review are reported to OMB in the Exhibits 300 submitted with the Fall IT Budget.

The PM Qualification Review will be replaced by a more stringent review process managed by the Department's Procurement Executive that meets new requirements described in OMB Office of Federal Procurement Policy Memorandum of April 25, 2007 entitled "The Federal

Acquisition Certification for Program and Project Managers." The new review process is expected to be implemented in late FY2008.

The following process diagram shows the sequential subprocessing for the existing Project Manager Qualification Review Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the following pages.

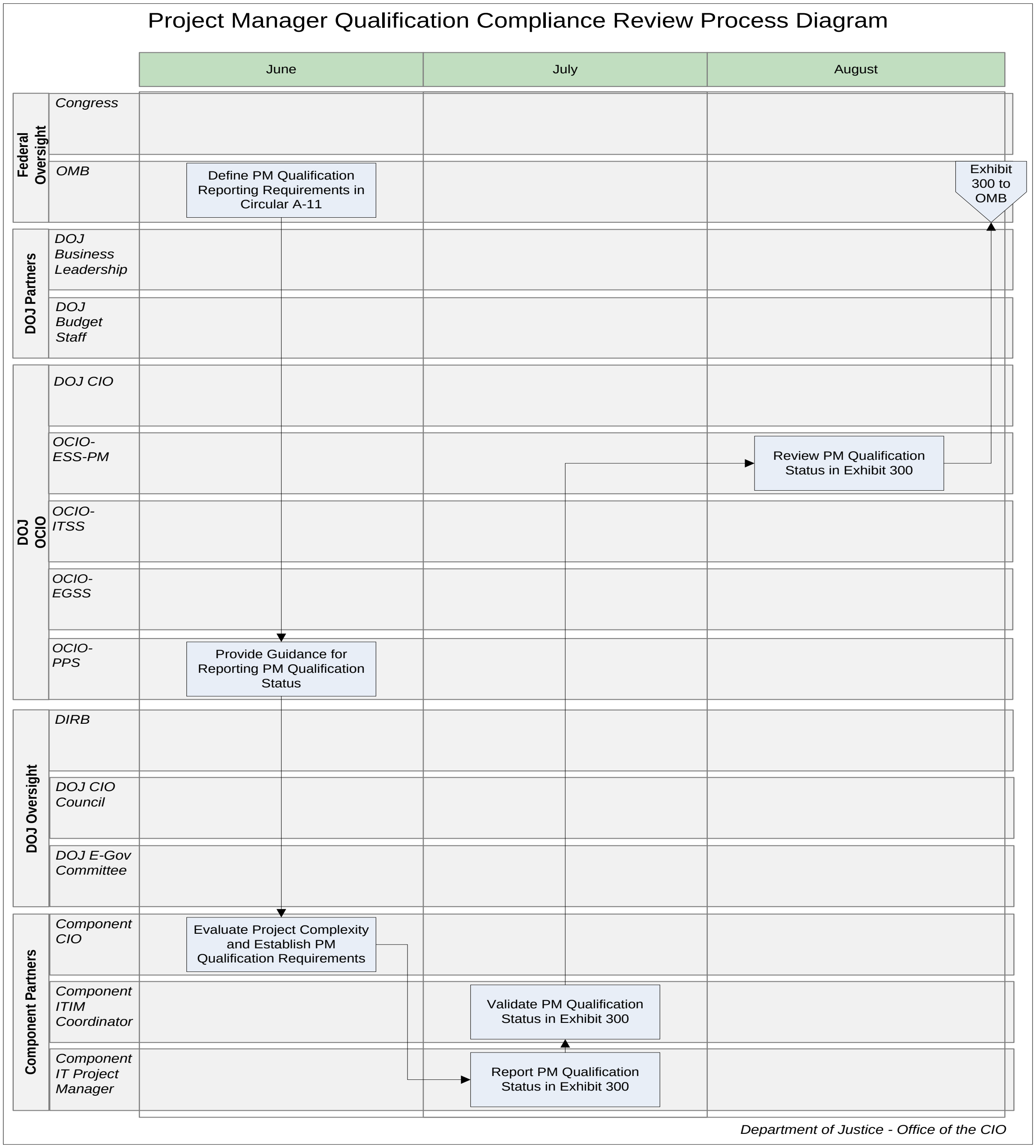

Project Manager Qualification Compliance Review Process Diagram
June
July
August
Federal Oversight
Congress
OMB
Define PM Qualification Reporting Requirements in Circular A-11
Exhibit 300 to OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO
OCIO-ESS-PM
Review PM Qualification Status in Exhibit 300
OCIO-ITSS
OCIO-EGSS
OCIO-PPS
Provide Guidance for Reporting PM Qualification Status
DOJ Oversight
DIRB
DOJ CIO Council
DOJ E-Gov Committee
Component Partners
Component CIO
Evaluate Project Complexity and Establish PM Qualification Requirements
Component ITIM Coordinator
Validate PM Qualification Status in Exhibit 300
Component IT Project Manager
Report PM Qualification Status in Exhibit 300
Department of Justice - Office of the CIO

Figure 3-22. Project Manager Qualification Compliance Review Process Diagram.

Define PM Qualification Reporting Requirements in Circular A-11. OMB will:

- Define the requirements for reporting Project Manager qualification in Circular A-11.
- Identify the criteria to be used for assessing PM qualification and provide definitions of the various qualification stages, as well as training or experience equivalencies.

Provide Guidance for Reporting PM Qualification Status. The DOJ OCIO will:

- Provide guidance to Components for reporting PM qualifications as part of the instructions for preparing Exhibit 300.

Evaluate Project Complexity and Establish PM Qualification Requirements. The Component OCIO will:

- Use the guidance in the Federal IT Project Manager Guidance Matrix to assign levels of complexity to IT projects and establish qualification criteria for project managers.
- Assess the qualification status of Project Managers assigned to each investment using the appropriate qualification criteria from the matrix.

Report PM Qualification Status. The Component IT Project Manager will:

- Report PM qualification status in the Exhibit 300 according to the guidance provided by DOJ OCIO and OMB A-11.

Validate PM Qualification Status. The Component CIO will:

- Review the PM qualification status reported in Exhibit 300 and ensure that the PM qualifications reported satisfy the requirements in the Federal IT Project Manager Guidance Matrix and are supported by documented training and experience.

Review PM Qualification Status in Exhibit 300. The DOJ OCIO will:

- Review the PM qualification status reported in Exhibit 300 and confirm that the qualification information reported satisfies the requirements in the Federal IT Project Manager Guidance Matrix and can be supported by documented training and experience.
- Ensure that appropriate corrective actions are planned to satisfy training requirements for PMs who are not fully qualified according to the Federal IT Project Manager Guidance criteria.

Component Self-Governance. Component responsibilities for the Project Manager Qualification Review are:

- Evaluate the complexity of Component IT investments and assign a rating (i.e., Level 1, 2, or 3) to each investment using the criteria contained in the Federal IT Project Manager Guidance Matrix.
- Assess Project Manager qualification compliance and assign qualification ratings using the guidance provided by DOJ OCIO and contained in OMB Circular A-11.
- Report PM qualification status in Exhibit 300s and/or on the Component Exhibit 51/53, as required.
- Implement a Project Manager training process and monitor the completion of qualification requirements by Component IT Project Managers who are not fully qualified for their current assignment.

3.3.2.2 Enterprise Architecture (EA) Review

The Enterprise Architecture (EA) Review Process implements requirements contained in the OMB EA Assessment Framework and builds on OMB's FEA Practice Guidance.

The EA Review Process will be implemented incrementally during FY2008. Initially, the EA Review Process will focus on the investments that are being reviewed by the Department Investment Review Board (DIRB). The EA Review Process will support the DIRB reviews by providing an overall architectural status rating for the investment. The EA review will then be expanded to include all investments that are required to submit an Exhibit 300 business case to OMB.

The EA review will be conducted throughout the fiscal year to evaluate EA alignment status of selected investments, to ensure that they are proceeding according to plan and are still sound investments for the Department. The criteria used to evaluate EA alignment and the rating structure is described in detail in the EA Program Manager's User Guide (PMUG) distributed by the Department's EA Program Management Office. After an investment has been assigned an EA alignment rating of red or yellow, the DOJ EAPMO will notify the PM to mitigate any alignment issues. The investment will entail ongoing monitoring by the DOJ EAPMO until an EA rating of green is achieved. The EAPMO will provide EA status ratings for DIRB projects to be reported to the DIRB at each review. The products of the EA Review Process serve the following purposes:

- The EA rating indicates the investment's overall EA compatibility progress and alignment status.
- The ongoing monitoring activities, where applicable, reports the progress toward completing the mitigation activities required to address EA alignment deficiencies identified in the EA review.

The process diagram in Figure 3-23 shows the sequence of subprocesses for the EA Review Process and the swim lanes identify the stakeholder responsible for each sub-process. The sub-processes are described following the diagram.

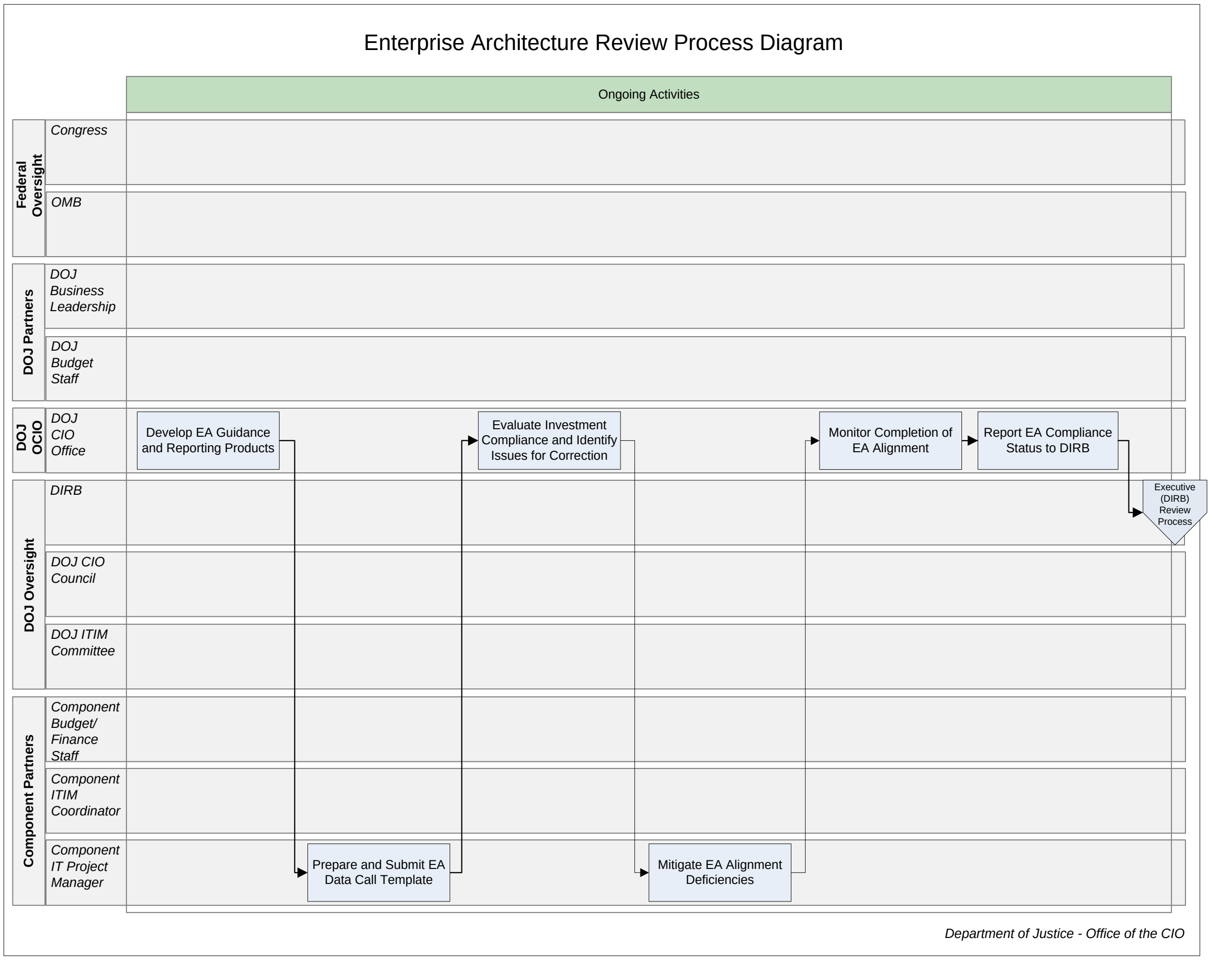

Enterprise Architecture Review Process Diagram
Ongoing Activities
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO Office
Develop EA Guidance and Reporting Products
Evaluate Investment Compliance and Identify Issues for Correction
Monitor Completion of EA Alignment
Report EA Compliance Status to DIRB
DOJ Oversight
DIRB
Executive (DIRB) Review Process
DOJ CIO Council
DOJ ITIM Committee
Component Partners
Component Budget/ Finance Staff
Component ITIM Coordinator
Component IT Project Manager
Prepare and Submit EA Data Call Template
Mitigate EA Alignment Deficiencies
Department of Justice - Office of the CIO

Figure 3-23. Enterprise Architecture Review Process Diagram

Develop EA Guidance and Reporting Products. The DOJ EAPMO will:

- Prepare a set of policy and EA guidance documents, to include the Transition and Sequencing Plan, As-Is and To-Be Architecture, Program Manager's User Guide and specific segment architecture documents to be used as references for Component and Department-level EA alignment and review.
- Prepare a data call template to gather relevant EA information for selected investments.

Prepare and Submit EA Data Call Template. The IT Project Manager will:

- Complete or update the EA Data Call template, in collaboration with the DOJ EAPMO. A detailed description of the data collected in the template is provided in the EA Program Manager's User Guide. NOTE: Investment performance information gathered for selected steady state and mixed life cycle investments with steady-state costs is used to support the Operational Analysis Review Process (Section 3.3.2.8)
- Submit the completed EA Data Call template to the DOJ EAPMO for review.

Evaluate Investment Compliance and Identify Issues for Correction. The DOJ EAPMO will:

- Review the completed EA data from Components using the EA evaluation criteria, and assign an EA alignment rating ranging from Green to Red. For a complete description of the EA review criteria, refer to the EA Program Manager's User Guide.
- Coordinate with Component level EA programs during the review to obtain any additional information on the investment being reviewed.
- Assign ratings of Yellow or Red to identify areas of weakness that must be corrected.

Mitigate EA Alignment Deficiencies. The IT Project Manager will:

- If necessary, work with DOJ EAPMO to address EA weaknesses rated Yellow or Red.
- Submit any changes or improvements to DOJ EAPMO for review and concurrence.

Monitor Completion of EA Alignment. The DOJ EAPMO will:

- Monitor progress against investment corrective action and evaluate the adequacy of actions to correct weaknesses.
- Report the progress of investments to the DOJ CIO.

Report EA Alignment Status to DIRB. The DOJ EAPMO will:

- Report EA alignment status for DIRB projects during scheduled DIRB reviews and report investment progress, if appropriate.

Component Self-Governance. Component responsibilities for the EA Review Process are:

- Evaluate Department-level investments managed within the Component using the Department's EA guidance and report the EA alignment of those investments to the Department EA and the appropriate segment architectures.

3.3.2.3 Acquisition Compliance Review

The Acquisition Review is performed by the OCIO Enterprise Solutions Staff. The review currently is used to ensure that OCIO-managed IT acquisitions leverage available Federal and Department software license agreements, GSA schedules and other blanket purchase agreements. The review is conducted as part of the procurement planning process that precedes the release of a solicitation for bids.

3.3.2.4 E-Government Compliance Review

The E-Government Compliance Review is conducted by the E-Government Services Staff Compliance Manager to ensure the Department complies with the stipulations of the E-Government Act of 2002 (Public Law 107-347l 44 U.S.C. Ch 36) and the associated OMB implementation guidance (OMB Memorandum 03-18, Implementation Guidance for the E-Government Act of 2002). The purpose of the review is to monitor the Department's progress in implementing/adopting the E-Gov solutions identified in the OMB-approved DOJ E-Government Implementation Plan. The E-Government Services Staff (EGSS) performs the review to monitor the timely and effective completion of the Plan milestones.

Projects selected for monitoring through the E-Gov Compliance Review include all the Department's investments that implement the President's Management Agenda for Expanding Electronic Government (E-Gov). These investments are identified in the OMB E-Gov Implementation Plan, with specific milestones for adopting the appropriate E-Gov/Lines of Business/SmartBuy initiatives and the transition away from and/or shut down of investments that duplicate these initiatives.

The E-Government Compliance review is conducted each quarter as part of the Department's quarterly E-Government progress report to OMB. Each quarter, OMB transmits a) an updated E-Gov Implementation Plan, which includes new milestones, existing milestones (not completed) and completed milestones; and b) a workbook template (E-Government Milestone Report) that lists only the milestones that need to be completed in the current quarter. DOJ actions to implement OMB approved E-Gov solutions/services are monitored to track the completion of scheduled milestones. The OMB-provided E-Government Milestone Report is updated and submitted to OMB at the end of the quarter to report the completion of plan milestones. A sample of the E-Government Milestone Report is shown in Appendix E.6.

The following process diagram shows the sequential subprocessing for the E-Gov Compliance Review Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the following pages.

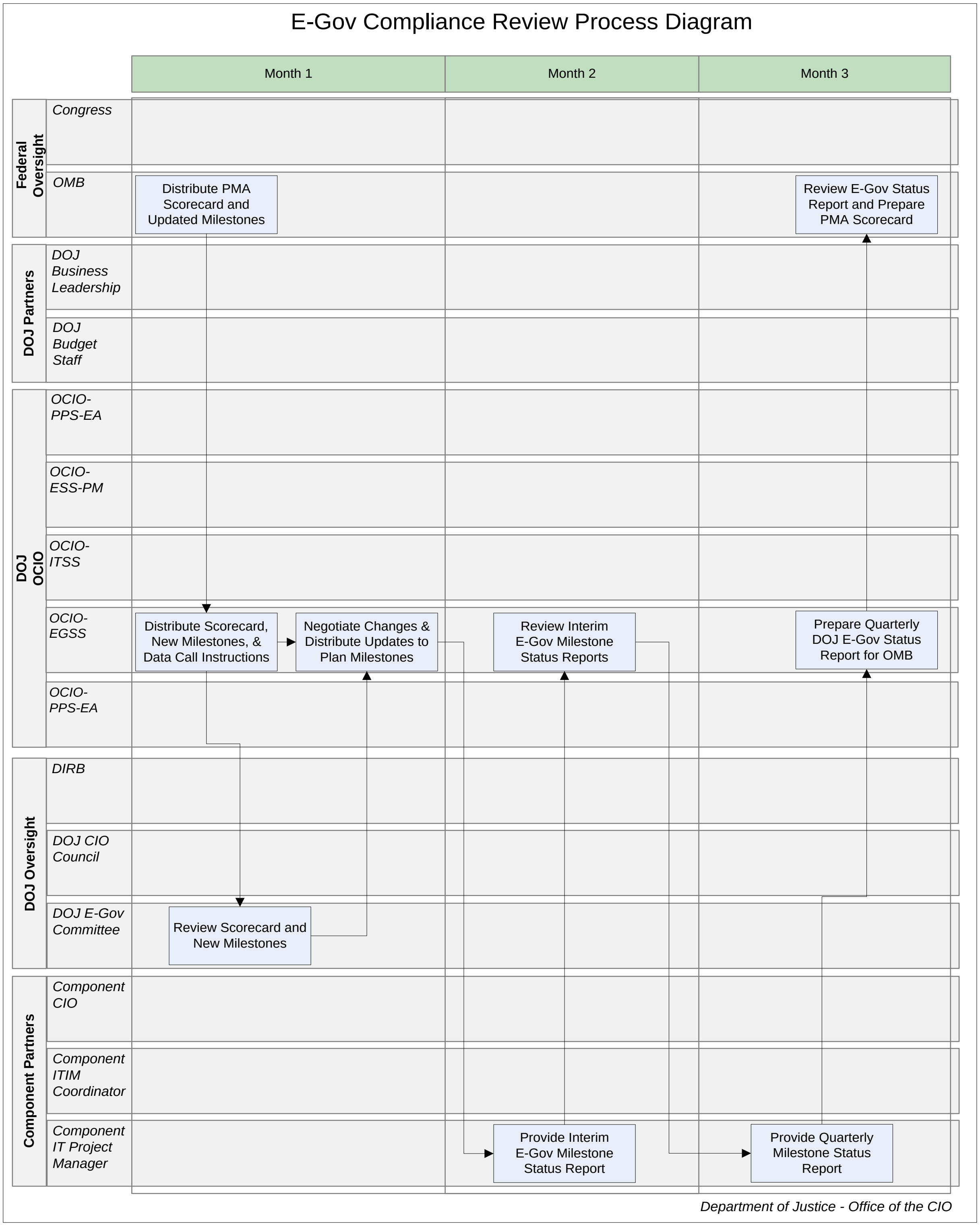

E-Gov Compliance Review Process Diagram
Month 1
Month 2
Month 3
Federal Oversight
Congress
OMB
Distribute PMA Scorecard and Updated Milestones
Review E-Gov Status Report and Prepare PMA Scorecard
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
OCIO-PPS-EA
OCIO-ESS-PM
OCIO-ITSS
OCIO-EGSS
Distribute Scorecard, New Milestones, & Data Call Instructions
Negotiate Changes & Distribute Updates to Plan Milestones
Review Interim E-Gov Milestone Status Reports
Prepare Quarterly DOJ E-Gov Status Report for OMB
OCIO-PPS-EA
DOJ Oversight
DIRB
DOJ CIO Council
DOJ E-Gov Committee
Review Scorecard and New Milestones
Component Partners
Component CIO
Component ITIM Coordinator
Component IT Project Manager
Provide Interim E-Gov Milestone Status Report
Provide Quarterly Milestone Status Report
Department of Justice - Office of the CIO

Figure 3-24. E-Gov Compliance Review Process Diagram.

Distribute PMA Scorecard and Updated Milestones. OMB will:

- On the first day of the quarter, distribute the PMA scorecard results from the previous quarter to all executive departments and agencies.

- Distribute the updated implementation plan milestones for the new quarter for DOJ review and concurrence

Distribute PMA Scorecard Results, New Milestones and Data Call Instructions. The DOJ OCIO will:

- On the first day of the quarter, distribute the following to all DOJ E-Gov Committee:
  - Scorecard from previous quarter.
  - Templates, guidance and instructions for any data calls, if applicable.
  - Milestones for new quarter based on the most recently approved implementation plan.

Review Scorecard and New Milestones. The DOJ E-Gov Committee will:

- Review the E-Gov Scorecard results from the previous quarter and the implementation milestones for the current quarter based on the most recently approved implementation plan.
- Address Component questions and identify milestones that may require changes to the approved implementation plan.

Negotiate Changes and Distribute Updates to Plan Milestones. The DOJ OCIO will:

- Review proposed changes to the implementation plan with DOJ E-Gov project leads.
- Review and discuss proposed changes with OMB.
- Concur with changes to the updated implementation plan based on mutual agreements.
- Inform the Component E-Gov POC and the DOJ E-Gov project leads of any changes to the milestones for the new quarter.

Provide Interim E-Gov Milestone Status Report. The Component E-Gov POC will:

- Provide an interim progress report mid-way through the quarter consisting of the following information:
  - If milestone is completed, evidence of completion must also be provided.
  - If milestone cannot be completed within the quarter, Component POC provides justification, as well as proposed date for milestone to be completed**.**

Review Interim E-Gov Milestone Status Report. The DOJ OCIO will:

- Review interim E-Gov reports from Components to monitor progress and identify problems.
- Work with appropriate points of contact to resolve or reschedule the completion of the milestones that are not progressing according to plan.

Provide E-Government Milestone Status Report. The Component E-Gov POC will**:**

- Report the status of completed milestones and transmit the status report to EGSS with evidence of completion 15 days before the end of the current quarter.

Prepare Quarterly DOJ E-Gov Status Report for OMB. The DOJ OCIO will:

- Collect final milestone status and evidence of completion information from Components.

- Prepare the quarterly E-Gov status report and submit the report to OMB not later than the last day of the quarter.

Review E-Gov Status Report and Prepare E-Gov Scorecard. OMB will:

- Review the Department’s E-Gov Milestone Report and assign a grade of Green, Yellow, or Red based on the progress with completing the quarterly milestones and implementing the DOJ E-Government Implementation Plan.
- Prepare the milestone plan for the next quarter.

Component Self-Governance. Component responsibilities for the E-Gov Compliance Review are:

- Identify Component representative to the DOJ E-Gov Committee (E-Gov Working Group) and ensure representative attends committee meetings.
- Identify the Component IT projects that are part of the DOJ E-Gov Implementation Plan.
- Monitor the progress of designated E-Gov projects to ensure compliance with the DOJ E-Gov Implementation Plan.
- Ensure Project Managers of designated E-Gov projects provide interim and quarterly milestone status reports as required.

3.3.2.5 IT Security Compliance Review

IT Security Compliance Reviews are conducted to ensure that the Department’s information systems are designed, developed, implemented and maintained in compliance with applicable laws, Department and Federal IT security policies and procedures and recognized best practices. Security reviews serve three primary purposes:

1) Ensure information system security requirements are adequately assessed and planned for during system development;
2) Periodically assess the adequacy and effectiveness of information system security measures; and
3) Assess the risks associated with security events, new threats and vulnerabilities.

Security reviews are conducted at Department, Component and system/project levels at specific stages of the System Development Life Cycle. For operational systems, the organization will assess all of the security controls in the information system during the accreditation life cycle and are triggered to occur according to three main scenarios:

I. A subset of controls is assessed annually. The subset selection is based on (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected by the organization to protect the information system; (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system; (iv) controls selected by the IT Security Council for a given year’s assessment (also known as authority to operate or ATO quality controls).

II. Volatile controls are assessed more frequently than once during the accreditation life cycle in accordance with their respective periodicity requirements identified in IT Security Standards and information system security plans.
III. When required to address security events, new threats and vulnerabilities.

A description of the IT Security Program, its goals, compliance activities and the roles and responsibilities for stakeholders can be found in the Department of Justice IT Security Program Management Plan, which is available via DOJNet on the ITSS Web Page or directly from the DOJ OCIO IT Security Staff. Because of the variety of security reviews and scenarios, it is difficult to illustrate the sequence of events on a single chart. The IT Security Program Management Plan describes the purpose, process and products for each compliance review, as well as the roles and responsibilities of all stakeholders. Key responsibilities for Department, Component and system stakeholders are highlighted below.

Key Department-level responsibilities:

- Department senior program officials are responsible for mission risk assessment resulting from operation of the information systems required to perform their missions; maintaining accurate information system inventory; and oversight of security weakness corrective action plans of actions and milestones.
- The OIG is responsible for conducting financial and FISMA audits to assess security controls for selected systems and overall IT security program implementation.
- The DOJ OCIO IT Security Staff (ITSS) is responsible for monitoring the compliance statistics for the systems and applications reported in the C&A Web IT Security Dashboard to identify specific problem areas for follow-up with appropriate C&A team members. ITSS also evaluates systemic program issues for action by the IT Security Council and performs OCIO targeted reviews of selected information systems annually.

Key Component-level responsibilities:

- Component configuration control boards are responsible for overseeing information system change management and security impact assessment.
- Component Authorizing Officials are responsible for ensuring information system risk management procedures are properly implemented.

Key system/project-level responsibilities:

- System and data owners and their information system security officers and managers are responsible for day-to-day operational oversight and continuous monitoring of information system security and risk posture.
- Information system owners are responsible for ensuring that information system configurations meet the Department’s minimum security requirements, that configuration monitoring is accomplished and that remediation actions are taken, as necessary, to comply with information system security control requirements.

The DOJ OCIO ITSS monitors the status of required and corrective actions for the Department’s non-intelligence community systems using the Department’s Cyber Security Assessment and Management (CSAM) Toolkit. The toolkit currently consists of C&A Web for SBU information systems and TrustedAgent for classified systems. The TrustedAgent tool will be retired once the classified version of C&A Web is accredited. The C&A Web and TrustedAgent tools provide a variety of management reports to facilitate the assessment and management of information system security and associated program risk and they also generate compliance statistics for quarterly and annual FISMA reports. The C&A Web IT Security Dashboard also provides key metrics for selected IT Security Program goals for operational information systems.

A sample Security System Summary Report produced from CSAM is shown in Appendix E.7 to illustrate the information monitored in each of the nine assessment areas.

3.3.2.6 Privacy Compliance Review

The Privacy Compliance Review is coordinated jointly by Privacy Compliance Managers from the OCIO E-Government Services Staff and by the DOJ Privacy and Civil Liberties Office (PCLO). The review consists of three parts: a technical review performed by OCIO to ensure that the Privacy Impact Assessment is technically accurate; a privacy review performed by PCLO to ensure privacy issues are addressed adequately; and if needed, a legal review, performed by JMD's Office of General Counsel (OGC), to ensure any legal issues have been addressed properly. The reviews are to be performed during the initial development of new investments to ensure privacy issues are addressed and whenever major changes are approved for operational systems to ensure any new privacy issues are identified, addressed and mitigated. The OCIO and PCLO jointly monitor the status of the review, approval and when required, the posting of IT system Privacy Impact Assessments (PIAs). The Privacy Compliance status for investments is tracked using the IT Security Staff C&A Web IT Security Dashboard and is reported to OMB through the FISMA compliance reporting process.

The following process diagram shows the sequential subprocessing for the Privacy Compliance Review Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the following pages.

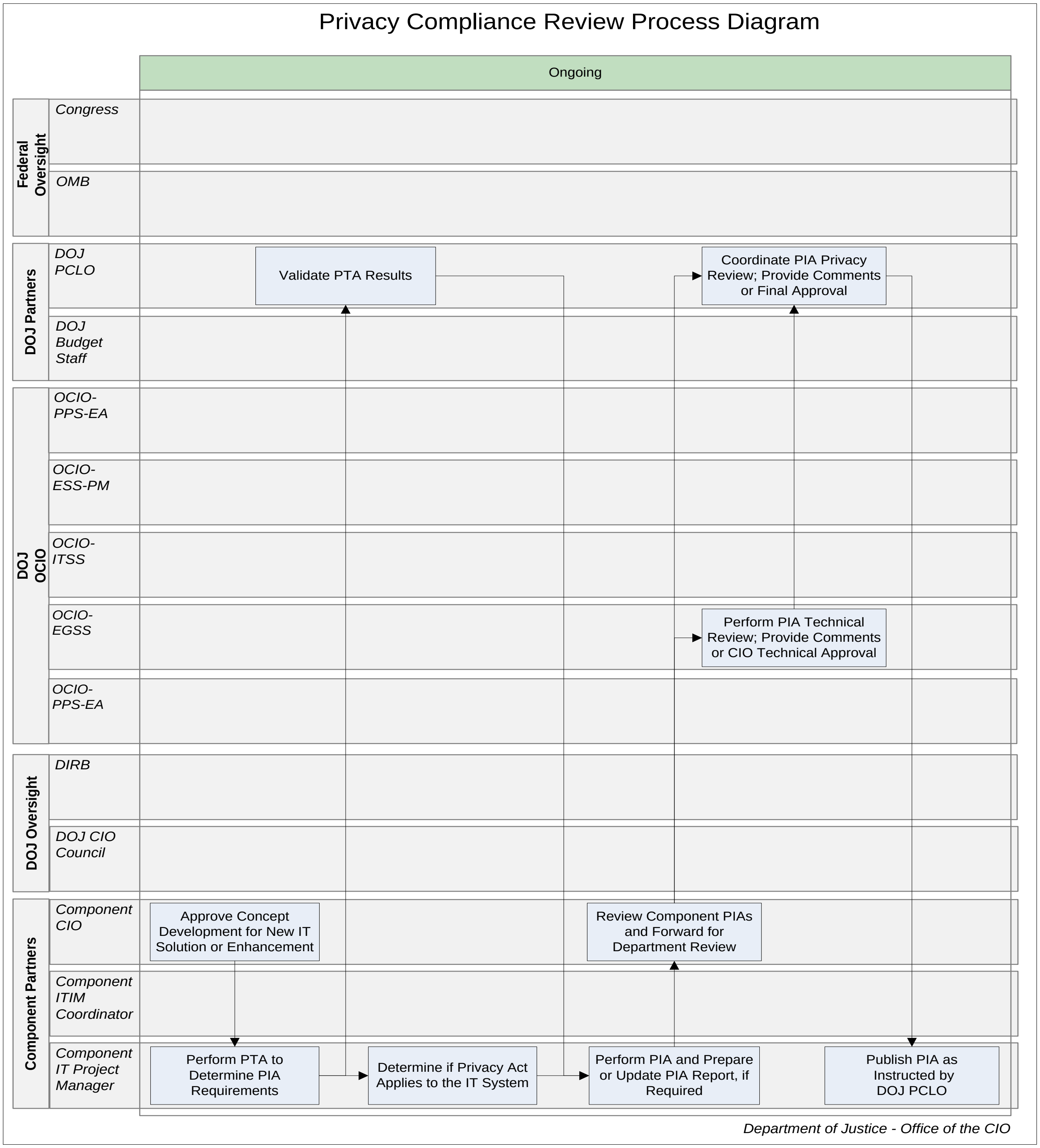

Privacy Compliance Review Process Diagram
Ongoing
Federal Oversight
Congress
OMB
DOJ Partners
DOJ PCLO
DOJ Budget Staff
DOJ OCIO
OCIO-PPS-EA
OCIO-ESS-PM
OCIO-ITSS
OCIO-EGSS
OCIO-PPS-EA
DOJ Oversight
DIRB
DOJ CIO Council
Component Partners
Component CIO
Component ITIM Coordinator
Component IT Project Manager
Validate PTA Results
Coordinate PIA Privacy Review; Provide Comments or Final Approval
Perform PIA Technical Review; Provide Comments or CIO Technical Approval
Approve Concept Development for New IT Solution or Enhancement
Review Component PIAs and Forward for Department Review
Perform PTA to Determine PIA Requirements
Determine if Privacy Act Applies to the IT System
Perform PIA and Prepare or Update PIA Report, if Required
Publish PIA as Instructed by DOJ PCLO
Department of Justice - Office of the CIO

Figure 3-25. Privacy Compliance Review Process Diagram.

Approve Concept Development for New IT Solution or Enhancement. The Component CIO will:

- Review proposals for new IT solutions or enhancements to existing systems and approve development of concepts based on Component mission and business priorities.

Perform PTA to Determine PIA Requirements. The Component IT Project Manager will ensure that the following actions occur:

- Perform the Privacy Threshold Assessment described in the DOJ Privacy Impact Assessments Official Guidance.
- Upload the PTA into Trusted Agent and complete all applicable fields in the privacy section of Trusted Agent.
- Based on the results of the PTA, determine if a new PIA, or an update to an existing PIA is required. If determination is made that no PIA or PIA update is required, no further action is required.

Validate PTA Results. The Department PCLO will:

- Review and validate the results of the PTA in Trusted Agent.
- Notify the Component if a PIA must be completed, regardless of the PTA results.

Determine if Privacy Act applies to the IT system. The Component IT Project Manager will ensure that the following actions occur:

- Work with the Senior Component Official for Privacy and/or PCLO to determine if the Privacy Act applies to the IT system. When the Privacy Act applies, determine whether a System of Records Notice (SORN) must be created or if the system is covered by existing Component, Departmental or Government-wide SORNs.
- Complete all applicable SORN fields in the privacy section of Trusted Agent.

Perform PIA and Prepare or Update the PIA Report, if Required. The Component IT Manager will ensure that the following actions occur:

- Perform a Privacy Impact Assessment in accordance with the DOJ Privacy Impact Assessments Official Guidance.
- Prepare a complete PIA report for new investments, or update the applicable sections of the existing PIA to address new privacy issues associated with system changes.
- Submit the PIA for review and approval within the Component and incorporate changes as required.
- After the PIA has been reviewed and approved within the Component, submit the PIA for Department-level review and approval by DOJ CIO and DOJ PCLO. Also load the PIA into the DOJ OCIO CSAM/Trusted Agent system.
- Incorporate changes identified from Department-level review.

Review Component PIAs and Forward for Department Review. Component CIOs will:

- Review Component PIAs for technical accuracy and coordinate privacy review by the Senior Component Official for Privacy or other component privacy expert.
- Provide comments for improving the PIA to the IT Project Manager, if necessary.
- Forward approved Component PIAs to DOJ OCIO and DOJ PCLO for Department-level review and approval.

Perform PIA Technical Review; Provide Comments or CIO Technical Approval. The DOJ CIO will:

- Review the Component PIA for technical accuracy and adequacy in describing the safeguards and mitigations of threats to protecting information in identifiable form.

- Provide comments for improving the PIA, or issue technical approval and forward comments or approval to the DOJ PCLO.

Coordinate PIA Privacy Review; Provide Comments or Final Approval. The DOJ PCLO will:

- Review the PIA to ensure the assessment addresses all the appropriate issues regarding protection of information in identifiable form for the system or the enhancement.
- Coordinate a review of privacy issues by the DOJ Office of General Counsel (OGC), when required.
- Collect comments from the DOJ CIO technical review and OGC privacy review, when required and provide the comments to the Component for revision of the PIA, if required.
- Issue final approval for the PIA and provide publication instructions to the Component.

Publish PIA as Instructed by the DOJ PCLO. The Component IT Project Manager will ensure that the following action occurs:

- Publish the PIA for public access as instructed by the DOJ PCLO.

Component Self-Governance. Component responsibilities for the Privacy Compliance Review are:

- Assess all new IT systems or enhancements to existing systems for privacy impacts.
- Coordinate technical and privacy reviews of PIAs within Components before submitting for Department review.
- Ensure PIAs for all Component IT systems are reviewed periodically to ensure they are up to date with latest policy, security standards and privacy laws.

3.3.2.7 Cost/Schedule/Risk Compliance Review

The Cost/Schedule/Risk (C/S/R) Review, previously known as the CIO Dashboard review, is managed by the Enterprise Solutions Staff Compliance Manager. The review process implements requirements defined by OMB for monitoring IT project cost, schedule and performance and for improving IT project planning and execution. These requirements are defined in OMB memorandum M-04-24 entitled "Expanded Electronic Government (e-Gov) President's Management Agenda (PMA) Scorecard Cost, Schedule and Performance Standard for Success" and OMB Memorandum M-05-23 entitled "Improving Information Technology (IT) Project Planning and Execution" and are implemented in DOJ Information Resources Management Policy DOJ Order 2880.1B. The C/S/R review process provides the DOJ CIO, DOJ Component CIOs and project managers of selected IT projects with a "quick reference" on the current cost, schedule, performance and risks for important and highly visible DOJ IT projects. The C/S/R review examines these selected IT projects to ensure they are being managed within acceptable cost, schedule and risk thresholds. Projects are selected annually for review using the following criteria:

- All projects being monitored by the DIRB.
- All projects that are required to submit an Exhibit 300 to OMB.
- Other important projects selected by the DOJ CIO.

The C/S/R review is also used to monitor earned value data for projects that must comply with the Earned Value Management System (EVMS) requirements of ANSI/EIA-748. These projects include:

- Information Technology (IT) projects with development/modernization/enhancement (DME) costs that exceed $10M annually or $25M over a five year life cycle period.
- IT projects requiring the special attention of the DOJ CIO due to high management visibility, level of DME funding, duration of the development phase, or level of risk.

Once a project is selected for the C/S/R review, the Project Manager must provide project baseline information including target cost, project schedule and milestones and risk information for the DOJ CIO Project Dashboard. Project progress (i.e., cost, schedule and risk status) must then be recorded in the Dashboard each month for review by the OCIO Enterprise Solutions Staff Compliance Manager. A detailed Project Status Report is produced for each project reviewed. Projects that report cost or schedule variances outside acceptable thresholds (± 5% or greater) are examined to determine root causes of the variance and identify the corrective actions being taken or planned by the Project Manager. The status of these non-compliant projects is briefed to the DOJ CIO and additional corrective actions may be assigned, if necessary.

The process diagram in Figure 3-26 shows the sequence of subprocesses for the Cost/Schedule/Risk Review Process and the swim lanes identify the stakeholder responsible for each sub-process. The sub-processes are described following the diagram.

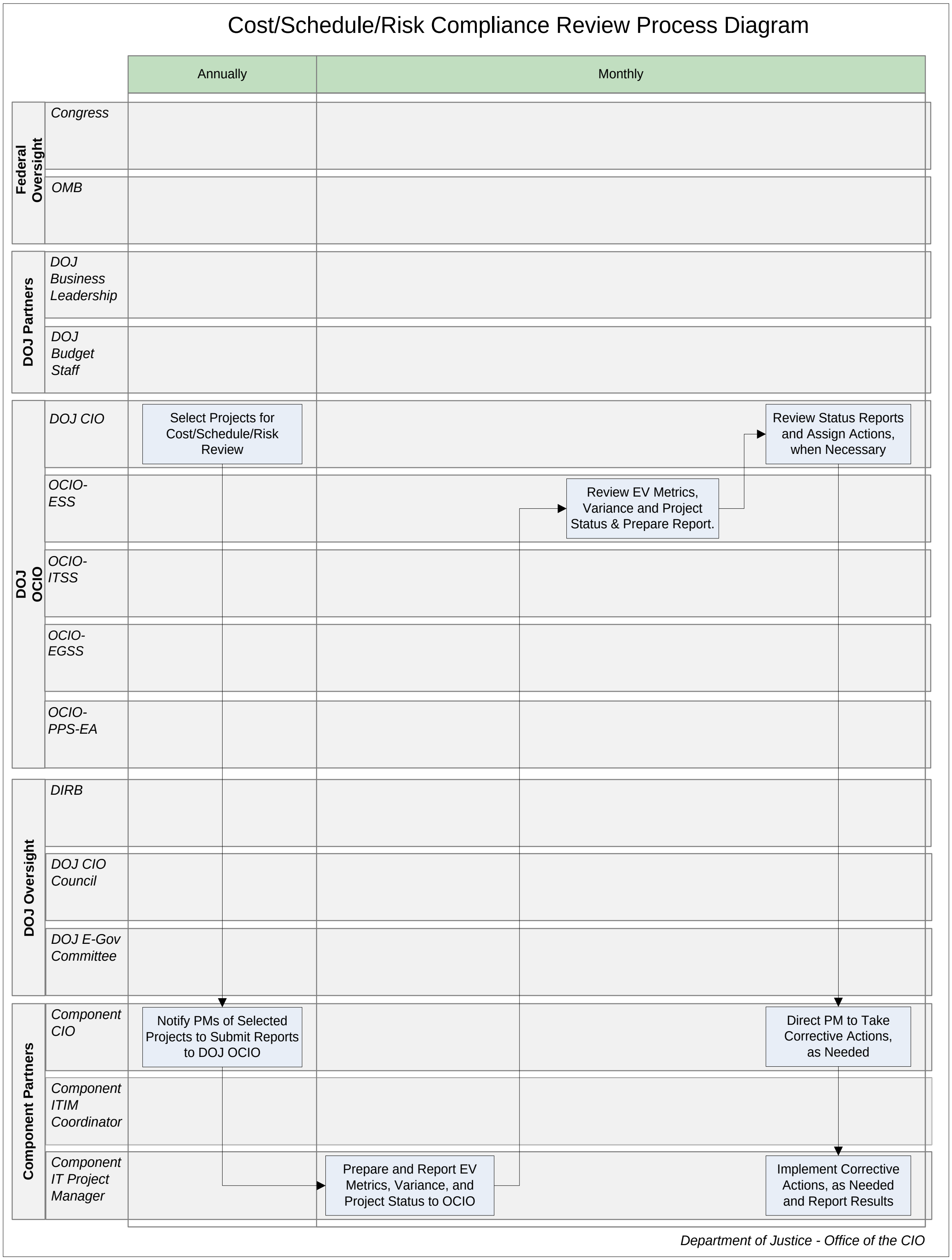

Cost/Schedule/Risk Compliance Review Process Diagram
Annually
Monthly
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO
OCIO-ESS
OCIO-ITSS
OCIO-EGSS
OCIO-PPS-EA
DOJ Oversight
DIRB
DOJ CIO Council
DOJ E-Gov Committee
Component Partners
Component CIO
Component ITIM Coordinator
Component IT Project Manager
Select Projects for Cost/Schedule/Risk Review
Notify PMs of Selected Projects to Submit Reports to DOJ OCIO
Prepare and Report EV Metrics, Variance, and Project Status to OCIO
Review EV Metrics, Variance and Project Status & Prepare Report.
Review Status Reports and Assign Actions, when Necessary
Direct PM to Take Corrective Actions, as Needed
Implement Corrective Actions, as Needed and Report Results
Department of Justice - Office of the CIO

Figure 3-26. Cost/Schedule/Risk Compliance Review Process Diagram.

Select Projects for Cost/Schedule/Risk Review. The DOJ OCIO will:

- Review the list of ongoing development projects and prepare a list of projects recommended to submit monthly C/S/R reports to the DOJ CIO Project Dashboard.
- Identify projects that must implement or maintain EVM systems that are compliant with ANSI/EIA-748 standard.
- Review the list of projects with the DOJ CIO to obtain a final list of projects that must report via the DOJ CIO Project Dashboard.
- Notify Components of the projects selected for Dashboard reporting for the coming fiscal year.

Direct PMs of Selected Projects to Submit Reports to DOJ OCIO. Component CIOs will:

- Notify the PMs of projects selected for Department-level C/S/R review and direct them to submit reports according to the DOJ CIO Project Dashboard instructions.

Prepare and Report EV Metrics, Variance and Project Status to DOJ OCIO. The IT Project Manager will:

- Enter the key milestones that will be completed during the fiscal year, the top five risks for the project and the funding for the project.
- Prepare EV metrics, conduct variance analysis and project status information monthly as specified by DOJ OCIO.
- Report the project EV, variance and project status information to the DOJ OCIO Project Dashboard not later than the 10th business day of the month. Information required includes: cost and schedule variance reports for variances that are greater than 5 percent; revised and/or actual start and completion dates for key project milestones; and updated status of the top five project risks.

Review EV Metrics, Variance and Project Status and Prepare Report. The DOJ OCIO will:

- Review the monthly EV metrics, validate the variance analysis reported by the Project Manager and review the project risk status.
- Prepare a Project Status Report that details the project EV status, discusses any corrective actions being taken or planned by the Project Manager and identify any additional actions that are recommended. A sample report is shown in Appendix D.5.
- Brief the contents of the report to the DOJ CIO.

Review Status Report and Assign Actions, when Necessary. The DOJ CIO will:

- Review the Project Status Report, evaluate the adequacy of any corrective actions taken by the Project Manager.
- Discuss the status of projects with variance outside acceptable limits with the appropriate Component CIO and assign additional corrective actions, when necessary.

Direct PM to Take Corrective Actions, as Needed. The Component CIO will:

- Direct the Project Manager to take corrective actions determined by the DOJ CIO.
- Monitor corrective action completion and evaluate results.

Implement Corrective Actions, as Needed and Report Results. The Component IT Project Manager will:

- Implement specified corrective actions and report completion.
- Report results of corrective actions.

Component Self-Governance. Component responsibilities for the C/S/R Review Process are:

- Monitor the progress of projects selected for Department C/S/R Review.
- Create a similar cost/schedule/risk review process for monitoring the status of important Component-level DME projects.

3.3.2.8 Operational Analysis Review

Operational analysis is a method of examining the ongoing performance of an information technology (IT) system and measuring that performance against established cost and performance targets. The DOJ operational analysis review process is designed to determine if the Department's important mixed life cycle projects and operational IT systems:

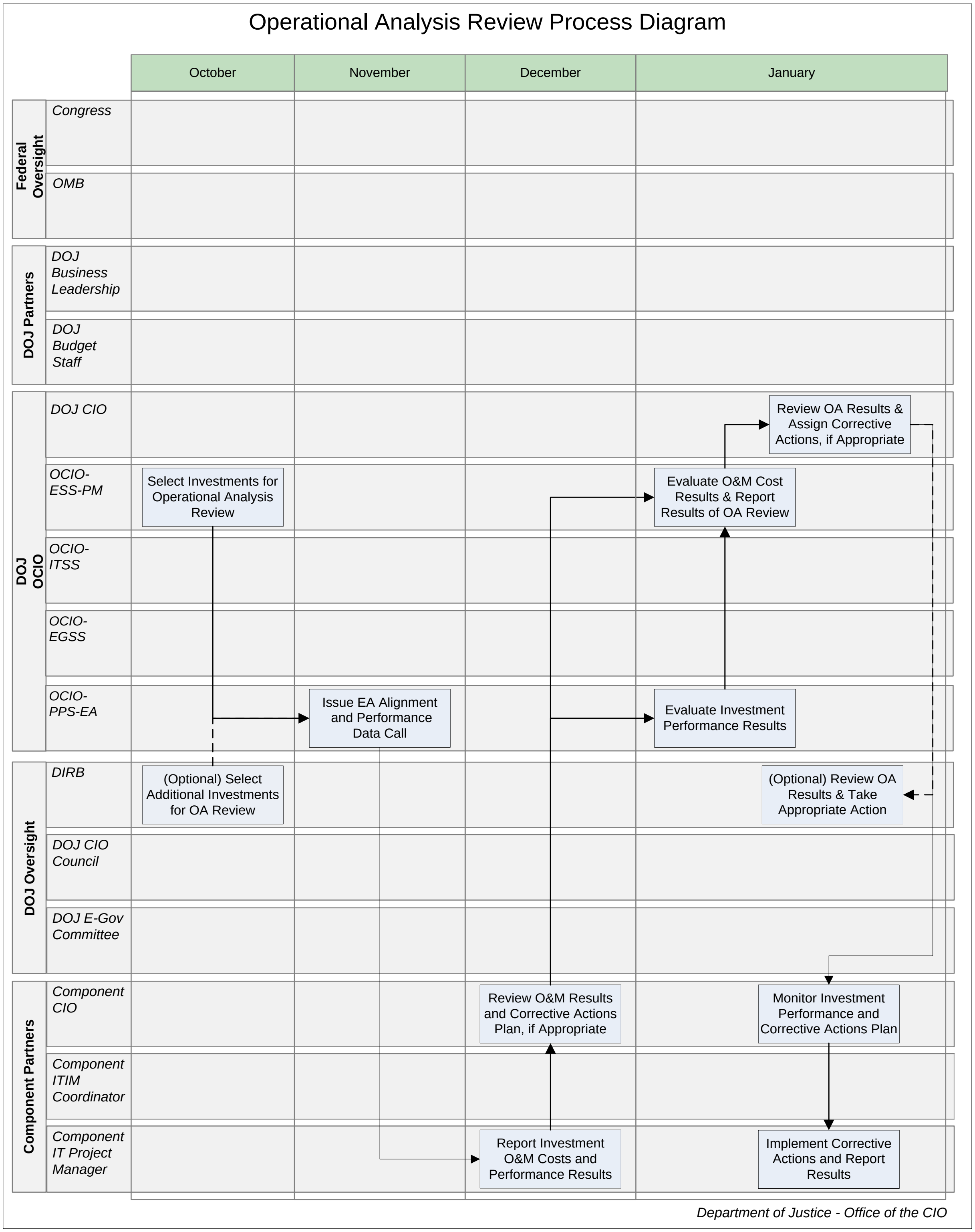
- are delivering the expected mission or business performance and improvement;
- are operating and can be maintained within the approved budget according to the system operations plan and
- are expected to meet the projected needs for the planned life cycle of the system.

Operational analysis reviews will be conducted annually on all mixed lifecycle IT investments and steady state systems that are required to submit an Exhibit 300 to OMB with the Department's budget and on other mixed lifecycle and steady state investments specifically selected by the Department IT Investment Review Board (DIRB).
Data used to conduct the annual operational analysis review consists of the following information for the most recently completed fiscal year:

- Performance data that compares the actual system performance results against the target business improvement and technical performance.
- Cost data that compares the actual O&M cost against the planned O&M cost.

When the cost or performance data reveals that investments achieved less than 90 percent of the performance target or exceeded the planned O&M cost target by more than 10 percent, Project Managers will determine the cause(s) for the variance, identify appropriate corrective actions and implement a plan of action to correct the deviations and return the investment to acceptable cost and/or performance limits. Component CIOs and the DOJ CIO will review the operational analysis results and concur with the PM's corrective action plan or identify additional corrective actions, if appropriate.

The following process diagram shows the sequential subprocessing for the Operational Analysis Review Process and the swim lanes show the stakeholder responsible for each sub-process. The sub-processes are described on the pages following the process diagram.


Operational Analysis Review Process Diagram
October
November
December
January
Federal Oversight
Congress
OMB
DOJ Partners
DOJ Business Leadership
DOJ Budget Staff
DOJ OCIO
DOJ CIO
OCIO-ESS-PM
OCIO-ITSS
OCIO-EGSS
OCIO-PPS-EA
DOJ Oversight
DIRB
DOJ CIO Council
DOJ E-Gov Committee
Component Partners
Component CIO
Component ITIM Coordinator
Component IT Project Manager
Select Investments for Operational Analysis Review
(Optional) Select Additional Investments for OA Review
Issue EA Alignment and Performance Data Call
Report Investment O&M Costs and Performance Results
Review O&M Results and Corrective Actions Plan, if Appropriate
Evaluate Investment Performance Results
Evaluate O&M Cost Results & Report Results of OA Review
Review OA Results & Assign Corrective Actions, if Appropriate
(Optional) Review OA Results & Take Appropriate Action
Monitor Investment Performance and Corrective Actions Plan
Implement Corrective Actions and Report Results

Department of Justice - Office of the CIO

Figure 3-27. Operational Analysis Compliance Review Process Diagram

Select Investments for Operational Analysis Review. The DOJ OCIO will:

- Select the investments for Operational Analysis review by identifying all mixed lifecycle or steady state investments that must submit an Exhibit 300 to OMB.
- Inform the Component IT Project Managers for all investments selected that an Operational Analysis review will be conducted on the investment and provide instructions for reporting the required information.

(Optional) Select Additional Investments for OA Review. The DIRB may:

- Select additional mixed lifecycle or steady state investments for Operational Analysis review based on high cost, high visibility, or poor performance, when appropriate.

Issue EA Alignment and Performance Data Call. The DOJ OCIO EAPMO will:

- Issue the EA alignment and performance data call to the project managers of selected IT investments. This data call is described in the Enterprise Architecture Compliance Review Process.

Report Investment O&M Costs and Performance Results. The Component IT Project Manager will:

- Determine the operations and maintenance (O&M) cost and performance results for the investment and compare the results against the target cost and performance goals.
- Report the results of the cost and performance review per instructions in the Exhibit 300 and in the EA data call.
- Submit the results for Component-level review and forwarding to the DOJ OCIO.
- When the investment performance results are less than 90 percent of the target performance or when actual O&M cost exceeds the target cost by more than 10 percent, determine the cause(s) for the variance and identify corrective actions to be implemented to remedy the cause.

Review O&M Results and Corrective Actions Plans, if Appropriate. The Component CIO will:

- Review the O&M cost and performance results for selected mixed lifecycle and steady state investments.
- Review the PM’s corrective actions plan, if appropriate and concur with the plan or identify additional corrective actions to be incorporated into the plan.
- Forward the O&M cost and performance results to DOJ OCIO for review.

Evaluate Investment Performance Results. The DOJ OCIO EAPMO will:

- Collect investment performance data as part of the EA Compliance Review process.
- Compare investment performance results to the target performance to identify investments that did not achieve at least 90 percent of target performance.
- Review the PM’s corrective action plan for any investment not achieving at least 90 percent of target performance and concur with the plan or identify additional actions that should be taken.

Evaluate O&M Cost Results & Report Results of OA Review. The DOJ OCIO will:

- Review the O&M cost results reported for each selected investment and compare the actual cost results against the original projected cost target to identify investments that exceeded the O&M cost target by more than 10 percent.
- Obtain investment performance data from OCIO EAPMO and compare investment performance results to O&M cost results.
- Review the PM corrective action plan for investments that exceeded the O&M cost target by more than 10% and concur with the plan or identify additional actions that should be taken.
- Report the results of the Operational Analysis review for each selected investment to the DOJ CIO and provide recommendations for additional corrective actions for incorporation into PM corrective action plans, if appropriate.

Review OA Results and Assign Corrective Actions, if Appropriate. The DOJ CIO will:

- Review the OA cost and performance results for all selected investments.
- If appropriate, assign additional corrective actions for investments that do not achieve at least 90 percent of target performance or that had actual O&M costs that exceeded the O&M cost target by more than 10 percent and communicate the corrective action requirements to the Component CIO responsible for the affected investment.
- Refer specific investments that are not meeting performance or cost targets to the DIRB for review, if appropriate.

(Optional) Review OA Results and Take Appropriate Action. The DIRB may:

- Review the O&M cost and performance results and the results of corrective actions for investments selected for DIRB review.
- Assign corrective actions as appropriate to initiate improvement, replacement, or termination of investments that are not delivering acceptable value versus cost.

Monitor Investment Performance and Corrective Actions Plan. The Component CIO will:

- Direct the PM to take corrective actions as assigned by the DOJ CIO or DIRB, if appropriate.
- Monitor investment performance and the progress of the PM corrective actions plan to ensure the desired results are achieved.

Implement Corrective Actions and Report Results. The IT Project Manager will:

- Plan and implement assigned corrective actions.
- Report progress and results to the Component CIO and DOJ CIO, as directed.

Component Self-Governance. Component responsibilities for the Operational Analysis Review are:

- Establish O&M cost and performance targets for selected Department-level mixed lifecycle and steady state investments.
- Report actual O&M cost and performance results as directed by OCIO.
- Implement a similar process for monitoring the O&M costs and performance of important Component-level mixed lifecycle and steady state investments.

Appendix A – DOJ Components

ATF – Bureau of Alcohol, Tobacco, Firearms and Explosives

ATR – Antitrust Division

BOP – Bureau of Prisons

CIV – Civil Division

COPS – Community Oriented Policing Services

CRM – Criminal Division

CRS – Community Relations Service

CRT – Civil Rights Division

DEA – Drug Enforcement Administration

ENRD – Environmental and Natural Resources Division

EOIR – Executive Office for Immigration Review

EOUST – Executive Office for U.S. Trustees

FBI – Federal Bureau of Investigation

***FCSC** – Foreign Claims Settlement Commission

FPI – Federal Prison Industries

JMD – Justice Management Division

NDIC – National Drug Intelligence Center

NSD – National Security Division

***ODR** – Office of Dispute Resolution

OFDT – Office of the Federal Detention Trustee

***OPA** – Office of Public Affairs

OIG – Office of the Inspector General

***OIP** – Office of Information and Privacy

***OIPL** – Office of Intergovernmental and Public Liaison

OJP – Office of Justice Programs

***OLC** – Office of Legal Counsel

***OLA** – Office of Legislative Affairs

***OLP** – Office of Legal Policy

***OPA** – Office of the Pardon Attorney

***OPR** – Office of Professional Responsibility

***OSG** – Office of the Solicitor General

***OVW** – Office on Violence Against Women

***PRAO** – Professional Responsibility Advisory Office

TAX – Tax Division

USA – United States Attorneys

USMS – United States Marshals Service

USNCB – U.S. National Central Bureau - Interpol

USPC – U.S. Parole Commission

***** Components that do not directly manage IT services or investments. These Components are not expected to implement the IT self-governance processes described in this guide.

Appendix B – Explanation of the Definition of IT for DOJ

According to the Clinger-Cohen Act of 1996 Information Technology (IT) is defined as "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the [Department]. 'Information technology' includes computers, ancillary equipment, software, software maintenance and support, firmware and similar procedures, services (including support services) and related resources."

In order to understand and apply the IT definition above, OCIO is issuing this explanation to add clarity on what is considered IT to ensure full and consistent reporting across the Department. Information Technology at the Department of Justice, that supports its wide and diverse mission and goals, are composed of three broad areas; Mission-Delivery and Business Solutions; IT Infrastructure and IT Practices and Management.

- **Mission-Delivery and Business Solutions** are comprised of software applications, systems, services and the people, processes, commercial contracts, overhead occupancy and technology that are used to acquire, manage, manipulate, display and compile information and data in direct and indirect support of the mission of the Department. Mission-Delivery and Business Solutions provide support for the missions of the Department as stated in the DOJ Strategic Plan which are:
    1. Prevent Terrorism and Promote the Nation's Security
    2. Prevent Crime, Enforce Federal Laws and Represent the Rights and Interests of the American People
    3. Ensure the Fair and Efficient Administration of Justice

  These strategic goals are advanced through core mission functions as noted in the IT Strategic Plan. These core functions are listed here with an illustrative example of an IT investment in that area:
    - Intelligence Operations
        - An example of this is the Component "ABC" investment in IT systems that collect data by audio, telephone, microphone telecommunications intercepts and other electronic surveillance methods in support of its intelligence and counter-terrorism mission.
        - Another example is the Component "ABC" investment in IT systems that are used in detection, identification, tracking and assessment of individuals and entities that pose threats to the United States and its interests.
    - Law Enforcement and Investigations
        - An example would be Component "ABC" investment in a system that provides electronic case, records, workflow, evidence management, case tracking and records search and reporting capabilities to be used for the collection and sharing of investigative data.
        - An example of this would be Component "ABC" investment in an IT system that maintains a record, inventory and catalog of improvised Explosive Devices used to support forensic examination.
    - Litigation and Judicial Activities
        - An example of this would be a case management system used by a component to support the management and administration of the legal cases it is involved with.
    - Correctional Activities

  - An example of this would be Component "ABC" investment in a mission support system used real-time to manage and report all inmate information such as work assignments that is critical to the safe and orderly operation of all federal prisons.
- Justice Program Coordination
  - An example of this would be Component "ABC" investment in a system that provides automated support for the application, approval, tracking and closeout of federal grant funds.
- Justice Information Services
  - An example of this would be Component "ABC" investment in a system that provides fingerprint identification services for local, state, federal and international law enforcement community and homeland security.
- Regulatory Activities
  - An example of this would be Component "ABC" investment in an IT system that tracks and reports interstate cigarette sales information.

These Core Mission Segments are assisted by support functions. They are listed here with an illustrative example:

- Administrative Management such as tracking systems, correspondence management, training or records management.
  - An example of this is the Component "ABC" investment in a correspondence management system used to support the executive office of the Department.
- Financial Management systems and related functions such as accounting, payroll, personnel, procurement and property management application systems.
  - An example of this is the Component "ABC" investment in an information system that supports the accounting functions of the Component.
- E-Gov contributions, assessments and service fees
  - These are the costs levied against DOJ for partner resource funding contributions and service fees for the federal e-government initiatives and lines of businesses. These are accounted for at the Department level on behalf of all components.

- **IT Infrastructure** is the people, processes, commercial contracts, overhead occupancy and technology used to interconnect computers and users and automate business processes. Infrastructure is also used to acquire process, store, send, receive, interchange, manage, switch, transmit and receive electronic data and information. IT Infrastructure includes:
  - **End User Systems and Support -** includes the people, processes, commercial contracts, overhead occupancy and technology necessary to enable and support an end user in their interaction with information technology services. The titles and terminology used in this section are drawn directly from the E-Government Information Technology Infrastructure Line of Business (ITI LoB). Examples include
    - **Client Hardware** (desktops, mobile, handheld devices)
    - **Peripheral Hardware** (local printers, shared printers)
    - **IT Management Hardware** (hardware supporting an IS process such as IT management client devices and IT management servers that support testing and training, network management, or asset management)
    - **User Client software** (PC operating systems, personal productivity, personnel database, messaging and groupware)
    - **IT Management Software (**of end user systems and support) (e.g., client/server hardware and software used exclusively for supporting IS functions such as network, systems storage, asset management, testing and training.)

        - **Occupancy (**fully burdened costs for the facilities being used by the staff such as space, furniture and utilities, etc.)
        - **Personnel (FTE's) (**Fully burdened salaries and benefits for government FTE's that provide the following functions: technical services, planning and process management, finance and administration and asset management.)
        - **Help Desk** (i.e. Hardware and software used for helpdesk support, government FTE's and commercial contract services and transmission telecommunications associated with the help desk function.)
    - **Mainframes and Server Systems and Support** – includes the people, processes, commercial contracts, overhead occupancy and technology to provide physical or logical, centralized or aggregated computer systems and related services to one or more parts of the enterprise(s). The titles and terminology used in this section are drawn directly from the E-Government ITI LoB. Examples include
        - **Mainframe systems and support** (e.g., IBM or compatible, or other)
        - **Server rooms and closets** (e.g., Wintel, Unix, Linux, other)
        - **Security Operations Command Centers**
        - **Data Center Operations and Disaster Recovery Facilities**
        - **Web hosting hardware and software operations** (licenses, maintenance, back up, disaster recovery)
        - **Electronic messaging** (e-mail, voice mail, video mail)
        - **Storage hardware and software operations** (licenses, maintenance, back up)
    - **Telecommunications Systems and Support -** includes the people, processes, commercial contracts, overhead occupancy and technology to provide "any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. The titles and terminology used in this section are drawn directly from the E-Government ITI LoB. Examples include:
        - **Network Operations Centers**
        - **Wire closets and cable management**
        - **Data Networks hardware and software**
        - **Telecommunications hardware and software**
        - **IPv6**
        - **Video hardware and software**
        - **Wireless communications**

      Telecommunications Systems and Support also includes such functions as: Wide Area Networks
        - Metropolitan Area Networks
        - Wide Area Networks
        - Local Area Networks
        - Internet Access
        - Wide Area Voice (Long Distance)
        - Local Area Voice (Phones, PBX) and
        - Video Teleconferencing.
    - **IT associated with Construction -** i.e. network cabling, wiring, or fiber optic infrastructure associated with facility construction - **SHOULD <u>NOT</u> BE REPORTED**

- **IT Practices and Management** are programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology and services not attributable to a specific mission-delivery/business solution or part of infrastructure. These programs and services support **<u>all</u>** the IT investments of the component. Some examples of what would be reported under IT Practices and Management include:

- Enterprise Architecture staff FTE's, systems and contracts supporting the Enterprise Architecture program for the component.
    - An example of this would be the "EA Program" investment of Component "ABC". This investment would account for the FTE resources for the staff of the EA program office, any contract costs that support this investment and any systems used by the program office to manage the program.
- IT Investment Management/Capital Planning and Investment Control staff FTE's, systems and contracts supporting the ITIM or CPIC program for the component. This could include related earned value management and IT governance activities as well.
    - An example of this would be the "IT Capital Planning" investment of Component "ABC. This investment would account for the FTE resources for the staff of the ITIM office, any systems used to manage and administer the ITIM program and any service costs in the form of commercial contracts to support the program.
- Information sharing activities of a general nature not attributable to a specific investment.
    - An example of this would be the "Information Sharing" investment that provides the common standards, data definitions and protocols to enable information to be shared across the Department and the larger Federal and State governments.
- IT Program Management staff FTE's, systems and contracts that support the IT program of the component as a whole. This could include such activities such as the records management, financial management, human resources management, IT training,
    - An example of this would be the "IT Program Management" investment of Component "ABC". This investment accounts for the immediate staff of the Office of the CIO, the budget officer for that office, the HR staff for that office, as well as any commercial contracts that are used to support the IT program as a whole of the component.
- IT Security Program – includes the people, processes, commercial contracts, overhead occupancy and technology used to manage the IT Security program of the component. Included here would be FTE's, systems and contract support to deliver this program. Specifically not included here are the IT security costs directly associated with a specific IT investment. Those costs should be reported as part of that investment.

An example of this would be the "IT Security" investment by Component "ABC" that accounts for the staff FTE's involved in managing the component IT security program and information system that it used to do that and a contract with a commercial service provider for contract help and technical expertise.

Appendix C – Legislative and Regulatory Requirements

All Federal agencies are required to perform IT investment management functions as stipulated by a variety of legislative acts, Federal regulations and executive policies. The following table identifies the most significant legislative and regulatory requirements that drive IT governance for the Department. The requirements are shown in the left column. The right column provides short descriptions of how this Guide addresses each requirement.

Legislative and Regulatory Requirements	IT Governance Guide
Consolidated Appropriations Act, 2008 : P.L. 110-161 states that:	Section 3.3.1 **Executive Review Process**
"None of the funds made available under this title shall be obligated or expended for Sentinel, or for any other major new or enhanced information technology program having total estimated development costs in excess of $100,000,000, unless the Deputy Attorney General and the investment review board certify to the Committees on Appropriations that the information technology program has appropriate program management and contractor oversight mechanisms in place and that the program is compatible with the enterprise architecture of the Department of Justice."	Describes the process for certify that projects meet the review requirements specified in P.L. 110-161.
Paperwork Reduction Act of 1995 requires executive agencies to:	Section 3.1.1 **IT Strategic Planning Process** Section 3.2 **IT Budget Phase**
Develop and maintain a strategic IRM plan.	Defines the process for developing and maintaining the IT strategic plan and describes how the plan guides IT investment and management decisions.
Develop and maintain a process to ensure IRM requirements are integrated with organizational planning, budget, financial management, human resources management and program decisions.	Describes the end-to-end process for identifying and evaluating IT investment requirements as an integrated part of organizational and program planning, budgeting and resource management.
Conduct formal training in information resources management.	Describes the training provided by DOJ OCIO to support Component participation in IT governance.
Clinger-Cohen Act of 1996 requires agencies to:	Section 3.0 **Governance Phases and Processes**
Design and implement a process for maximizing value and assessing and managing the risks of IT acquisitions and to define an IT architecture to guide IT investment. The process must provide for investment selection, management and evaluation of results.	Describes the IT governance processes and the criteria used for determining investment priorities and assessing investment return throughout the selection, control and evaluation processes.
E-Government Act of 2002 requires executive agencies to:	Section 3.3.2.4 **E-Government Compliance Review**
Support the efforts of OMB and GSA to develop, maintain and promote an internet-based system of delivering Federal Government information and services to the public.	Describes how E-Government Act requirements are integrated into the investment Compliance Review Process.
Develop performance measures that demonstrate how implementing electronic government enables progress toward agency goals, objectives and mandates.	Describes how performance measures are employed for evaluating IT investment value in supporting the Department's missions and goals.
Conduct Privacy Impact Assessments (PIA) for new IT investments and on-line information collections.	Describes the Department's PIA requirement as part of the IT governance life cycle.
Federal Information Security Management Act (FISMA) of 2002 requires agencies to:	Section 3.3.2.5 **IT Security Compliance Review**
Integrate information security processes with strategic and operational planning.	Describes how security requirements are considered during IT strategic and investment planning.

Legislative and Regulatory Requirements	IT Governance Guide
OMB Circular A-11 promulgates:	Section 3.2 **IT Budget Planning**
Instructions and formats for submitting IT budget requests and supporting exhibits (Exhibits 52, 53 and 300) as part of the Budget Formulation Process.	Describes how the Department collects, compiles, reviews and delivers the required budget exhibits to OMB as part of the IT governance process.
OMB Circular A-130 specifies IRM policy requirements for Federal executive agencies:	Section 3.2 **IT Budget Planning** Section 3.3.2.5 **IT Security Compliance Review**
Requires implementation of a capital planning and investment control (CPIC) process that links mission needs, information and information technology.	Describes the end-to-end CPIC process that links identification, selection and management of IT investments to mission needs and performance improvement.
Identifies required IRM documents including IRM strategic plan and IT capital plan.	Describes how the IT strategic plan and IT capital plan are developed, used and maintained within the IT governance life cycle.
Identifies the three components of IT capital planning and investment control and identifies evaluation actions that must be addressed in each component.	Describes the Department's three-phased IT governance life cycle which accomplishes the various evaluation activities identified in A-130.
Identifies linkages required between enterprise architecture and CPIC.	Describes the interactions of IT governance and enterprise architecture.
Specifies required IT security management actions.	Describes the IT security compliance review as a part of the investment Compliance Review Process.
GAO ITIM Framework:	Section 2.2 **Investment Life Cycle Model** Section 3.0 **Governance Phases and Processes**
Defines the 5 stage assessment framework used by GAO to determine the maturity of ITIM processes and operations within an organization.	Describes the management structures and processes the Department employs to implement a robust IT governance that maps to the GAO model.
OMB Memorandum M-03-22 dated September 26, 2003 requires executive agencies to:	Section 3.3.2.6 **Privacy Compliance Review**
Provides guidance to agencies for implementing the privacy provisions of the E-Government Act of 2002.	Describes the Privacy compliance review as a critical part of the Compliance Review Process.
OMB Memorandum M-05-23 dated August 4, 2005 requires executive agencies to:	Section 3.3.2.7 **Cost/Schedule/Risk Compliance Review**
Implement a plan for using EVMS to monitor major IT systems projects.	Describes the EVMS compliance review requirement for major developmental projects as part of the Compliance Review Process.
OMB Memorandum M-06-20 dated July 17, 2006 requires executive agencies to:	Section 3.3.2.5 **IT Security Compliance Review** Section 3.3.2.6 **Privacy Compliance Review**
Report FISMA and Privacy management program status on a quarterly basis as part of the President's Management Agenda (PMA) scorecard.	Includes these reporting requirements for the Department and Components as part of the Compliance Review Process.
Commerce-Justice-State Appropriations Act of 2006 requires the Attorney General to:	Section 2.2 **Investment Life Cycle Model** Section 3.2.1 **Spring IT Budget Planning Process** Section 3.3.1 **Executive Review Process**
Establish an investment review board chaired by the Deputy Attorney General to review IT investment progress and approve IT investments.	Defines the role of the Department IT Investment Review Board and describes the board's responsibilities for reviewing the progress of ongoing projects and approving IT investments.
Order DOJ 2880.1B, Information Resources Management:	Section 1.1 **Purpose**
Defines the Department IRM policies, identifies top level program requirements and delineates Component compliance requirements.	Serves as the companion document that describes how the Department's IRM policy is implemented and managed.

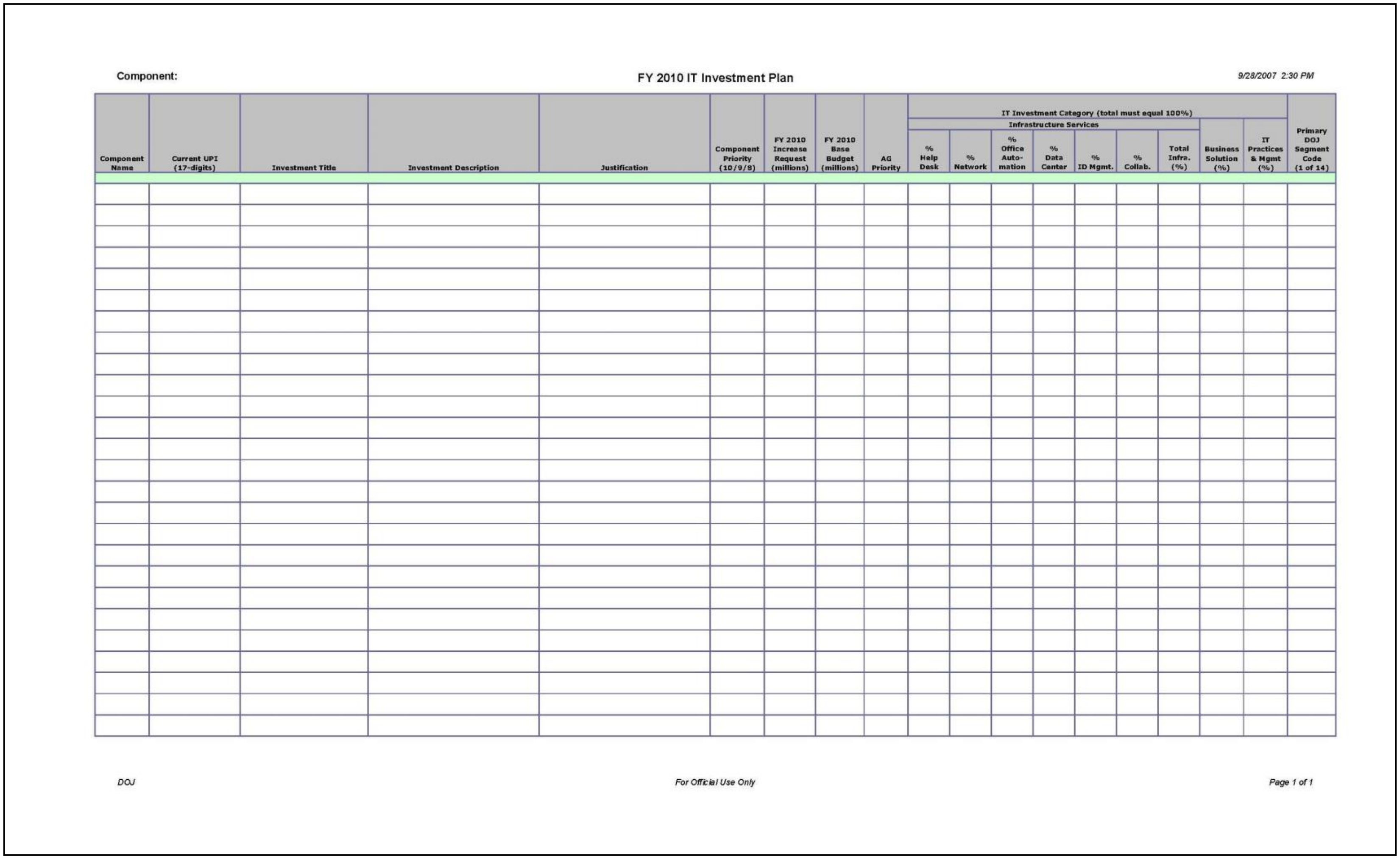
Appendix D – IT Budget Phase Products

A number of preformatted reports and investment evaluation tools are used during the IT Budget Phase processes to document investment proposals, budget requests and record the results of investment review. Descriptions of these products and instructions for obtaining usable copies of the corresponding templates are contained in this Appendix. The products include:

D.1 Component IT Investment Plan
D.2 Component Exhibit 51/53
D.3 OMB Exhibit 53 – Agency IT Portfolio Report
D.4 OMB Exhibit 300 – Capital Asset Plan and Business Case Summary
D.5 IT Budget Phase Scorecard
D.6 Exhibit 300 Evaluation Factors

D.1 Component IT Investment Plan

The Component IT Investment Plan is prepared by major and large IT investor Components during the IT Investment Planning Process to identify IT investment proposals being considered for inclusion in the upcoming budget planning cycle. The plan lists all new investments and enhancements to existing investments that are under consideration and provides a priority ranking for each investment proposal. The template for preparing the plan is distributed by the OCIO Policy and Planning Staff when the IT Investment Planning data call is announced. The template can also be downloaded from the OCIO Policy and Planning Staff webpage under ITIM on the DOJ CIO website on the DOJNet intranet. A sample template is shown in Figure D-1.



Component:

FY 2010 IT Investment Plan

9/28/2007 2:30 PM

									IT Investment Category (total must equal 100%)									
									Infrastructure Services									
Component Name	Current UPI (17-digits)	Investment Title	Investment Description	Justification	Component Priority (10/9/8)	FY 2010 Increase Request (millions)	FY 2010 Base Budget (millions)	AG Priority	% Help Desk	% Network	% Office Auto-mation	% Data Center	% ID Mgmt.	% Collab.	Total Infra. (%)	Business Solution (%)	IT Practices & Mgmt (%)	Primary DOJ Segment Code (1 of 14)

DOJ

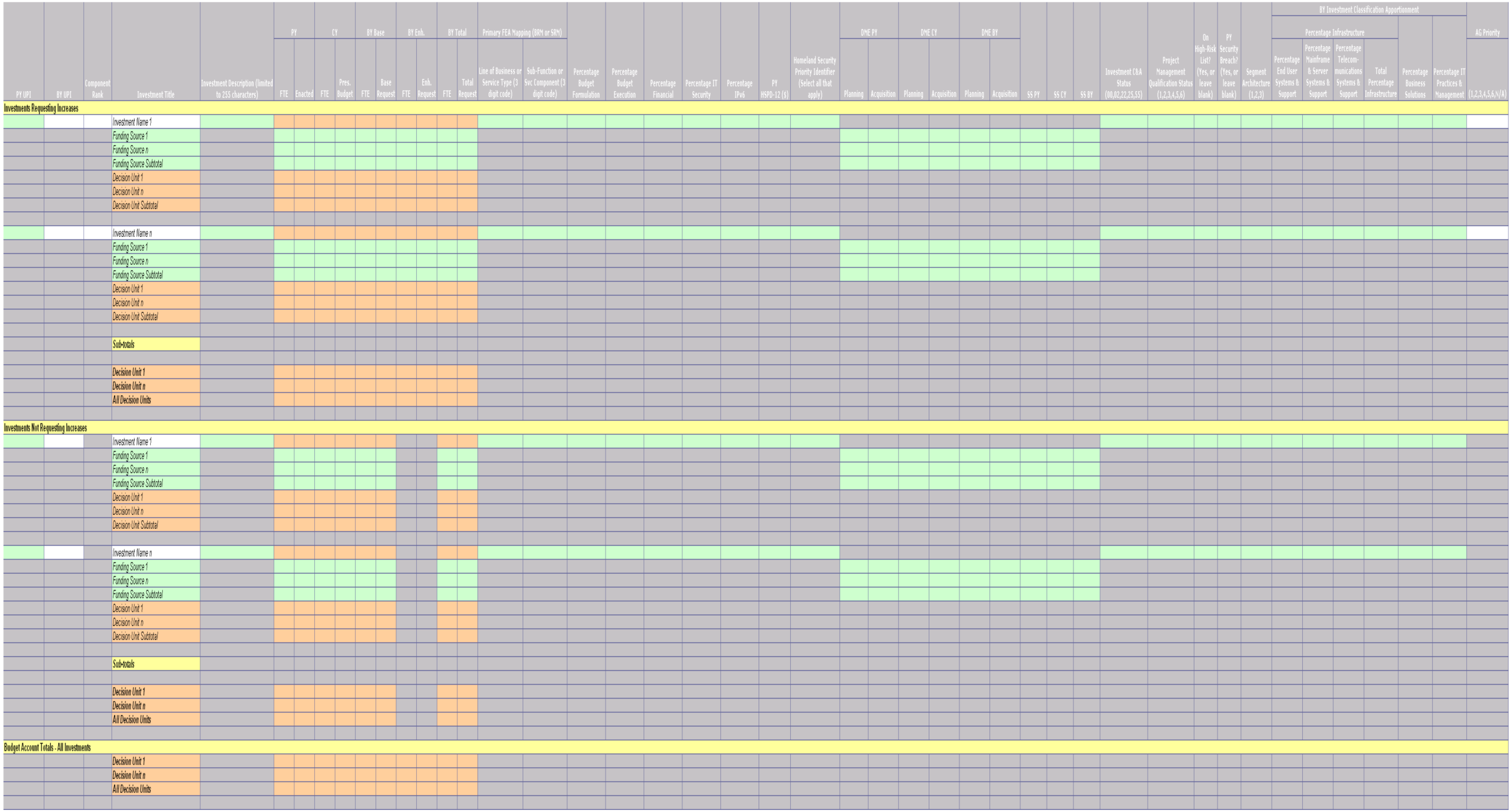
For Official Use Only

Page 1 of 1

Figure D-1. IT Investment Plan Template

D.2 Component Exhibit 51/53

The Component Exhibit 51/53 is a DOJ internal data collection tool prepared by each Component detailing the IT investment funds included in the Component Spring budget request, the OMB Passback and the President's Budget submissions. The Exhibit 51/53 template is jointly maintained by the DOJ Budget Staff and the DOJ OCIO and is distributed to Components with the Spring Budget Call. A sample of the Exhibit 51/53 form used during the FY2009 budget cycle is shown in Figure D-2.



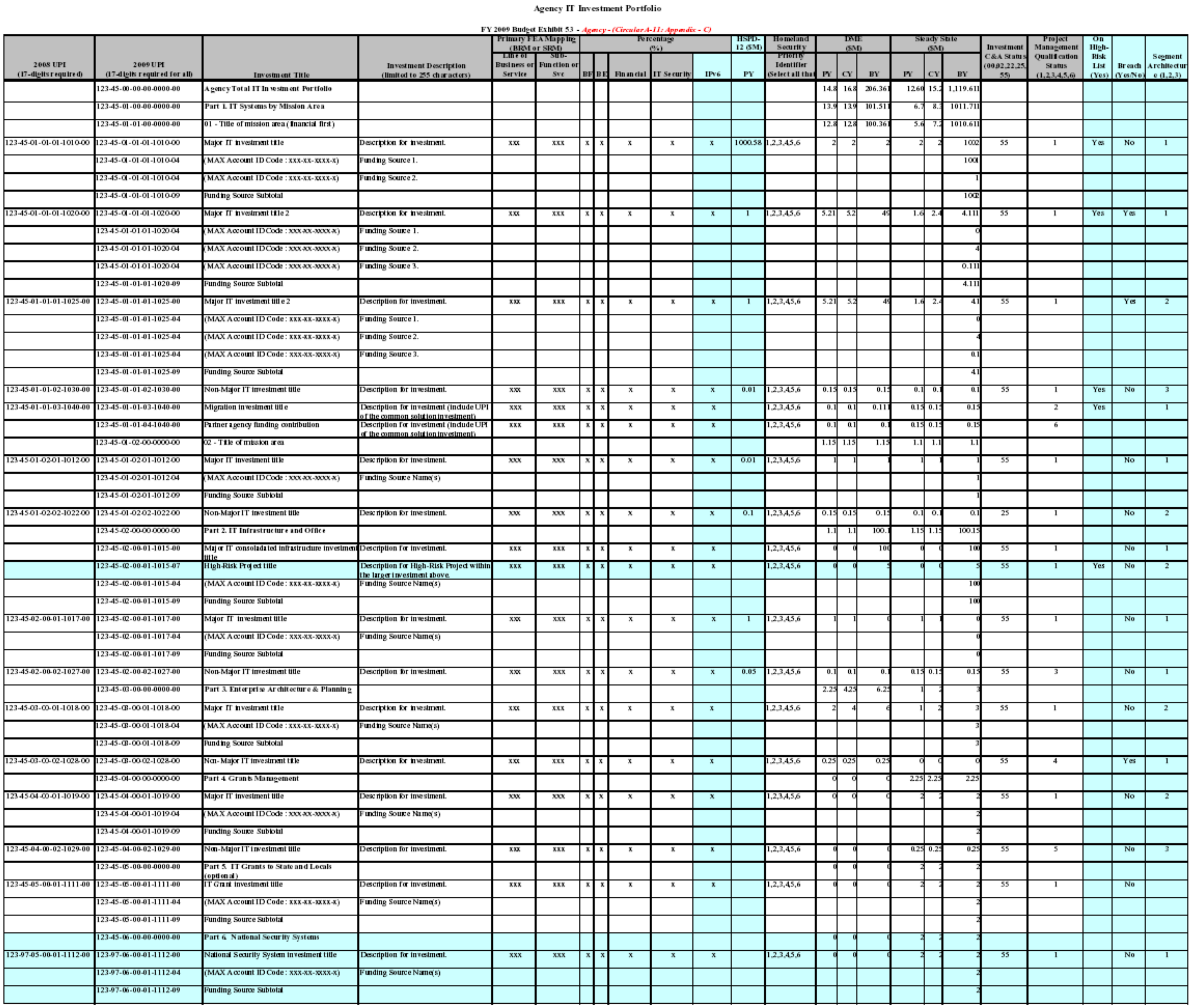
																																						BY Investment Classification Apportionment						
					PY		CY		BY Base		BY Enh.		BY Total		Primary FEA Mapping (BRM or SRM)									DME PY		DME CY		DME BY										Percentage Infrastructure						AG Priority
PY UPI	BY UPI	Component Rank	Investment Title	Investment Description (limited to 255 characters)	FTE	Enacted	FTE	Pres. Budget	FTE	Base Request	FTE	Enh. Request	FTE	Total Request	Line of Business or Service Type (3 digit code)	Sub-Function or Svc Component (3 digit code)	Percentage Budget Formulation	Percentage Budget Execution	Percentage Financial	Percentage IT Security	Percentage IPv6	PY HSPD-12 ($)	Homeland Security Priority Identifier (Select all that apply)	Planning	Acquisition	Planning	Acquisition	Planning	Acquisition	SS PY	SS CY	SS BY	Investment C&A Status (00,02,22,25,55)	Project Management Qualification Status (1,2,3,4,5,6)	On High-Risk List? (Yes, or leave blank)	PY Security Breach? (Yes, or leave blank)	Segment Architecture (1,2,3)	Percentage End User Systems & Support	Percentage Mainframe & Server Systems & Support	Percentage Telecom-munications Systems & Support	Total Percentage Infrastructure	Percentage Business Solutions	Percentage IT Practices & Management	(1,2,3,4,5,6,N/A)
Investments Requesting Increases																																												
			Investment Name 1																																									
			Funding Source 1																																									
			Funding Source n																																									
			Funding Source Subtotal																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			Decision Unit Subtotal																																									
			Investment Name n																																									
			Funding Source 1																																									
			Funding Source n																																									
			Funding Source Subtotal																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			Decision Unit Subtotal																																									
			Sub-totals																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			All Decision Units																																									
Investments Not Requesting Increases																																												
			Investment Name 1																																									
			Funding Source 1																																									
			Funding Source n																																									
			Funding Source Subtotal																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			Decision Unit Subtotal																																									
			Investment Name n																																									
			Funding Source 1																																									
			Funding Source n																																									
			Funding Source Subtotal																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			Decision Unit Subtotal																																									
			Sub-totals																																									
			Decision Unit 1																																									
			Decision Unit n																																									
			All Decision Units																																									
Budget Account Totals - All Investments																																												
			Decision Unit 1																																									
			Decision Unit n																																									
			All Decision Units																																									

Figure D-2. Component Exhibit 51/53

Blank Page

D.3 OMB Exhibit 53

The OMB Exhibit 53 Agency IT Portfolio Report lists all the IT investments requested for the Department and is submitted to OMB as the DOJ Fall IT Budget. The Exhibit 53 consolidates the investment information from Components into a single report for the Department. The content and use of Exhibit 53 is described in Section 53 of OMB Circular A-11. The current version of Circular A-11, which contains an example of Exhibit 53, is available for download at http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html . An example of the Exhibit 53 is shown in Figure D-3.



Agency IT Investment Portfolio

FY 2009 Budget Exhibit 53 - *Agency - (Circular A-11: Appendix - C)*

2008 UPI (17-digits required)	2009 UPI (17-digits required for all)	Investment Title	Investment Description (limited to 255 characters)	Primary FEA Mapping (BRM or SRM)		Percentage (%)					HSPD-12 ($M)	Homeland Security	DME ($M)			Steady State ($M)			Investment C&A Status (00,02,22,25, 55)	Project Management Qualification Status (1,2,3,4,5,6)	On High-Risk List (Yes)	Breach (Yes/No)	Segment Architecture (1,2,3)
				Line of Business or Service	Sub-Function or Svc	BF	BE	Financial	IT Security	IPv6	PY	Priority Identifier (Select all that	PY	CY	BY	PY	CY	BY					
	123-45-00-00-00-0000-00	Agency Total IT Investment Portfolio											14.8	16.8	206.361	12.60	15.2	1,119.611					
	123-45-01-00-00-0000-00	Part 1. IT Systems by Mission Area											13.9	13.9	101.511	6.7	8.3	1011.711					
	123-45-01-01-00-0000-00	01 - Title of mission area (financial first)											12.8	12.8	100.361	5.6	7.2	1010.611					
123-45-01-01-01-1010-00	123-45-01-01-01-1010-00	Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	1000.58	1,2,3,4,5,6	2	2	2	2	2	1002	55	1	Yes	No	1
	123-45-01-01-01-1010-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 1.															1001					
	123-45-01-01-01-1010-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 2.															1					
	123-45-01-01-01-1010-09	Funding Source Subtotal																1002					
123-45-01-01-01-1020-00	123-45-01-01-01-1020-00	Major IT investment title 2	Description for investment.	xxx	xxx	x	x	x	x	x	1	1,2,3,4,5,6	5.21	5.2	49	1.6	2.4	4.111	55	1	Yes	Yes	1
	123-45-01-01-01-1020-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 1.															0					
	123-45-01-01-01-1020-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 2.															4					
	123-45-01-01-01-1020-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 3.															0.111					
	123-45-01-01-01-1020-09	Funding Source Subtotal																4.111					
123-45-01-01-01-1025-00	123-45-01-01-01-1025-00	Major IT investment title 2	Description for investment.	xxx	xxx	x	x	x	x	x	1	1,2,3,4,5,6	5.21	5.2	49	1.6	2.4	41	55	1		Yes	2
	123-45-01-01-01-1025-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 1.															0					
	123-45-01-01-01-1025-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 2.															4					
	123-45-01-01-01-1025-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source 3.															0.1					
	123-45-01-01-01-1025-09	Funding Source Subtotal																41					
123-45-01-01-02-1030-00	123-45-01-01-02-1030-00	Non-Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	0.01	1,2,3,4,5,6	0.15	0.15	0.15	0.1	0.1	0.1	55	1	Yes	No	3
123-45-01-01-03-1040-00	123-45-01-01-03-1040-00	Migration investment title	Description for investment (include UPI of the common solution investment)	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0.1	0.1	0.111	0.15	0.15	0.15		2	Yes		1
	123-45-01-01-04-1040-00	Partner agency funding contribution	Description for investment (include UPI of the common solution investment)	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0.1	0.1	0.1	0.15	0.15	0.15		6			
	123-45-01-02-00-0000-00	02 - Title of mission area											1.15	1.15	1.15	1.1	1.1	1.1					
123-45-01-02-01-1012-00	123-45-01-02-01-1012-00	Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	0.01	1,2,3,4,5,6	1	1	1	1	1	1	55	1		No	1
	123-45-01-02-01-1012-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															1					
	123-45-01-02-01-1012-09	Funding Source Subtotal																1					
123-45-01-02-02-1022-00	123-45-01-02-02-1022-00	Non-Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	0.1	1,2,3,4,5,6	0.15	0.15	0.15	0.1	0.1	0.1	25	1		No	2
	123-45-02-00-00-0000-00	Part 2. IT Infrastructure and Office											1.1	1.1	100.1	1.15	1.15	100.15					
	123-45-02-00-01-1015-00	Major IT consoladated infrastructure investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	100	0	0	100	55	1		No	1
	123-45-02-00-01-1015-07	High-Risk Project title	Description for High-Risk Project within the larger investment above.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	5	0	0	5	55	1	Yes	No	2
	123-45-02-00-01-1015-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															100					
	123-45-02-00-01-1015-09	Funding Source Subtotal																100					
123-45-02-00-01-1017-00	123-45-02-00-01-1017-00	Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	1	1,2,3,4,5,6	1	1	0	1	1	0	55	1		No	1
	123-45-02-00-01-1017-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															0					
	123-45-02-00-01-1017-09	Funding Source Subtotal																0					
123-45-02-00-02-1027-00	123-45-02-00-02-1027-00	Non-Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x	0.05	1,2,3,4,5,6	0.1	0.1	0.1	0.15	0.15	0.15	55	3		No	1
	123-45-03-00-00-0000-00	Part 3. Enterprise Architecture & Planning											2.25	4.25	6.25	1	2	3					
123-45-03-00-01-1018-00	123-45-03-00-01-1018-00	Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	2	4	6	1	2	3	55	1		No	2
	123-45-03-00-01-1018-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															3					
	123-45-03-00-01-1018-09	Funding Source Subtotal																3					
123-45-03-00-02-1028-00	123-45-03-00-02-1028-00	Non-Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0.25	0.25	0.25	0	0	0	55	4		Yes	1
	123-45-04-00-00-0000-00	Part 4. Grants Management											0	0	0	2.25	2.25	2.25					
123-45-04-00-01-1019-00	123-45-04-00-01-1019-00	Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	0	2	2	2	55	1		No	2
	123-45-04-00-01-1019-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															2					
	123-45-04-00-01-1019-09	Funding Source Subtotal																2					
123-45-04-00-02-1029-00	123-45-04-00-02-1029-00	Non-Major IT investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	0	0.25	0.25	0.25	55	5		No	3
	123-45-05-00-00-0000-00	Part 5. IT Grants to State and Locals (optional)											0	0	0	2	2	2					
123-45-05-00-01-1111-00	123-45-05-00-01-1111-00	IT Grant investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	0	2	2	2	55	1		No	
	123-45-05-00-01-1111-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															2					
	123-45-05-00-01-1111-09	Funding Source Subtotal																2					
	123-45-06-00-00-0000-00	Part 6. National Security Systems											0	0	0	2	2	2					
123-97-05-00-01-1112-00	123-97-06-00-01-1112-00	National Security System investment title	Description for investment.	xxx	xxx	x	x	x	x	x		1,2,3,4,5,6	0	0	0	2	2	2	55	1		No	1
	123-97-06-00-01-1112-04	(MAX Account ID Code : xxx-xx-xxxx-x)	Funding Source Name(s)															2					
	123-97-06-00-01-1112-09	Funding Source Subtotal																2					

Figure D-3. Example OMB Exhibit 53

D.4 OMB Exhibit 300

The OMB Exhibit 300 Capital Asset Plan and Business Case Summary, commonly called the Exhibit 300, is used to provide a business case and project plan to OMB for selected investments. OMB distributes an updated version of the form each year as part of the update to OMB Circular A-11. The form and the instructions for completing it can be found in OMB Circular A-11, Section 300. It should be noted that only the parts of the form that apply to the specific project must be completed. A current version of OMB Circular A-11, including the Exhibit 300 form, is available for download on OMB's website at http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html .

D.5 IT Budget Phase Scorecard

The IT Budget Phase Scorecard is used to track Component compliance with the budget planning schedule and the degree of completeness of the information submitted during the course of the IT Budget Phase. The scorecard enables the DOJ OCIO to determine which Components are experiencing difficulties during the budget planning process so that corrective actions such as additional training, clarification of instructions or terminology, or other actions can be taken to improve the effectiveness of the process. A sample scorecard is shown in Figure D-4.

	ATF	ATR	BOP	CIV	COPS	CRM	CRS	CRT	DEA	ENRD	EOIR	EOUST	FBI	FEW	FPI	JMD	NDIC	NSD	ICDE	ODR	OFDT	OIG	OJP	OLC	OSG	TAX	USA	USMS	USNCB	USPC
Timeliness																														
Spring Call (May)																														
OMB Subm. (Aug)																														
Change (May->Aug)																														
Passback (Dec)																														
Change (Aug->Dec)																														
Completeness																														
Spring Call (May)																														
OMB Subm. (Aug)																														
Change (May->Aug)																														
Passback (Dec)																														
Change (Aug->Dec)																														
Overall																														
Score																														
Trend																														

Legend

Timeliness	***On Time (Green)***	?	***Completeness***	***> 95% Complete (Green)***	?	***Change/Trend***	***No Change***	?
	3 to 5 Days late (Yellow)	?		***> 80% Complete (Yellow)***	?		***Improving***	?
	> 5 Days Late (Red)	?		***< 80% Complete (Red)***	?		***Not Improving***	?
	Not Submitted (Tan)	?		***Not Submitted (Tan)***	?			

Figure D-4. IT Budget Phase Scorecard

D.6 Exhibit 300 Evaluation Factors

The OMB Exhibit 300 Capital Asset Plan and Business Case Summary is reviewed by the DOJ OCIO for completeness, accuracy and consistency before the exhibit is submitted to OMB as part of the Department's budget request package. The evaluation factors listed below are used by OCIO Compliance Managers to assess each Exhibit 300 in the following areas:

- Acquisition Strategy
- Alternatives Analysis
- Enterprise Architecture
- Performance Based Management System
- Life Cycle Cost Analysis
- Performance Information
- President's Management Agenda
- Privacy
- Project Management
- Risk Management
- Security

A. Acquisition Strategy Evaluation Factors

- Does the Acquisition Strategy adequately mitigate risks to the Federal Government?
- Does strategy use principles of performance based contracting?
- Is there evidence that Section 508 requirements are considered?
- Is earned value provided for those IT investments that require it?
- Is the Contracting Officer certified and qualified to conduct the acquisition?
- If earned value is not required or used is there an adequate explanation for each contract for which EA is not required?
- Does the response to Part 1.C. Question 2 adequately explain why certain contracts do not require earned value?

B. Alternatives Analysis Evaluation Factors

- Does the Alternatives Analysis include three viable alternatives? Note: do not count "Do nothing" or "Continue current operations" as one of the alternatives.
- Have the risk adjusted costs and benefits of each alternative been compared consistently using the same criteria for all the alternatives?
- Are the assumptions used in the analysis clearly described and documented?
- Is the basis for the solution choice clear and compelling?
- Are the specific qualitative benefits the investment will provide identified?
- If this investment will replace a legacy system is that system(s) identified and are the applicable UPI's and dates for replacement provided?
- Are legacy systems that will be retired by this investment identified if applicable.

C. Enterprise Architecture Evaluation Factors

- Is this investment:
  - Included in the agency's target EA?
  - Included in the agency's EA transition strategy? If yes, name it. If no, justify why it is not included.
- Is this investment identified in completed and approved segment architecture? If yes, name it.
- Does the investment leverage existing components/ applications across government and/or is it considered a component/ application provider, if applicable?
- Does the investment provide the public with access to a government automated information system? If so, what interface is required by the user?
- Complete SRM and TRM tables to the extent possible, given the lifecycle stage of the project.

D. Performance-Based Management System/Earned Value Management System Evaluation Factors

- How well are budgeted and actual costs accounted for, controlled and managed?
- Are cost and schedule variances computed? Are they used to monitor how well the investment is proceeding relative to its cost estimates? Are they used as a management tool?
- How well has the deployment of the initiative adhered to its original project cost and schedule?
- Are schedule slippages being properly managed?
- If the project is required to use the ANSI-standard EVMS, is that in place?

- If the project is in steady state is the required Operational Analysis process in place?

E. Performance Goals Evaluation Factors

- How Performance metric shows alignment between the execution of the investment against the overall performance of the Department
- Investment Alignment to the Performance Measurement Categories in the Performance Reference Model (PRM)
- Original baseline performance design goals
- Performance measures, indicators, or other metrics
- Reports on progress toward meeting and achieving original baseline or revised baseline goals or performance measures or indicators
  - Stated benefits from the alternatives in the Alternatives Analysis in Part II.A of the Exhibit 300?

F. President's Management Agenda Evaluation Factors

- Does the investment support one or more of the President's Management Agenda Initiatives?
- Does the investment achieve or improve Department mission effectiveness?
- Does the investment involve/use collaboration efforts (i.e., support one or multiple agencies, leverage existing or proposed investments, etc.)?
- Is each PMA initiative listed, addressed under Question 13.a?

G. Privacy Compliance Evaluation Factors

- Has a privacy threshold analysis been conducted?
- Have all privacy requirements for the investment been completed?
- Has the PIA, if required, been received and approved by the component, DOJ CIO and DOJ PCLO?
- Is the PIA publicly posted on DOJ PCLO web site?
- Is the SORN, if required, up-to-date and gone through all Departmental approvals?
- Has the SORN, if required, been published in the federal register?

H. Project Management Evaluation Factors

- Has a qualified/certified project manager been appointed
- Has the project level of complexity been evaluated?
- Has the project manager reviewed the Exhibit 300?
- Is a project budget and schedule in place?
- Is all of the necessary documentation, project team, plans, processes, security, resources and metrics in place to manage a sound program?
- Is risk an integral part of project management?
- Is management involved in project oversight and decision making as necessary
- Has all the PM contact information been provided?
- Is there an appropriate response to Question in Part I. Section A. Overview, Question 11.a regarding the qualifications of the project manager for the FAC-P/PM certification level?
- Is Part I, Section A, Question 24 regarding the GAO high risk area answered appropriately?

I. Risk Management Evaluation Factors

- Is there a comprehensive Risk Management Plan in place?
- Are the appropriate risks identified, quantified, evaluated and mitigated?
- Does risk appear to be managed throughout the life cycle of the investment?

- If there is no risk plan is there a strategy for managing risk articulated?

J. Security Management Evaluation Factors

- Has a comprehensive security analysis been conducted?
- Are all systems related to this investment properly identified and addressed in Table 3 systems in Planning and Table 4 systems in Operation as appropriate?
- Has security been addressed at the system/application level?
- Are the security controls in place consistent with all FISMA, FIPS, NIST and NSA Security Standards?
- Have all security requirements for the investment with respect to its life cycle phase been met?
- Are the security costs in line with the overall costs of the project outlined in the Summary of Spending table (Part I.A.)?
- Are all system category I breaches reported properly as reported by DOJCERT?

Appendix E – IT Oversight Phase Reports

This appendix provides descriptions and examples of many of the Department-level reports used in the IT Oversight Phase. Instructions for obtaining commonly used templates are included in the description, or examples are shown for purposes of illustration. The reports include:

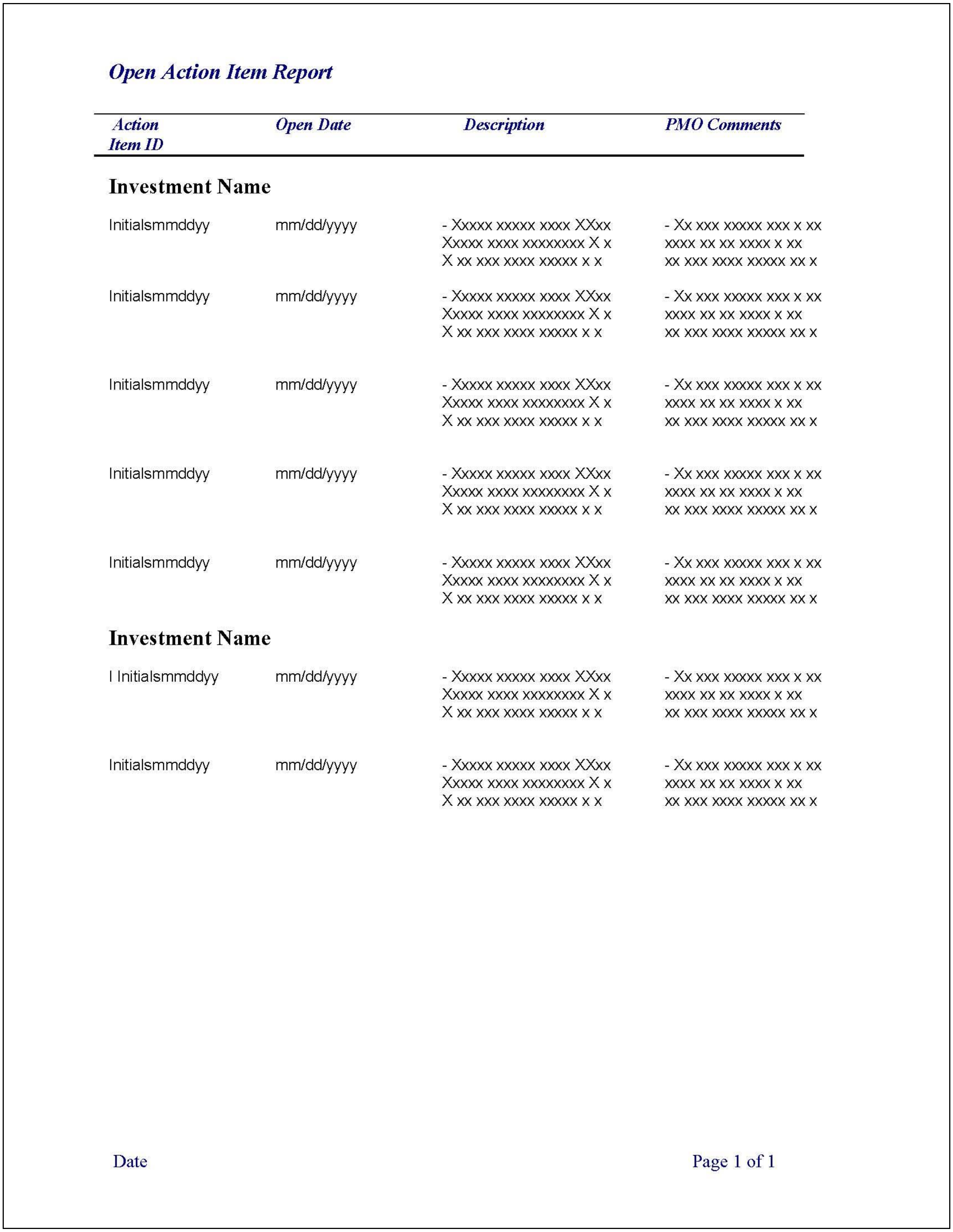
E.1 DIRB Open Action Item Report
E.2 DIRB Action Item History Report
E.3 DIRB Project Review Template
E.4 DIRB Meeting Summary
E.5 Cost / Schedule/ Risk Project Review Report
E.6 E-Government Implementation Milestone Report
E.7 IT Security Department System Summary Report
E.8 Compliance Report

E.1 DIRB Open Action Item Report

The DIRB Exec. Sec. prepares and maintains the DIRB Open Action Item Report to document and monitor the completion of action items assigned to Component IT Project Managers by the DIRB. It contains only the open action items assigned to one, many, or all projects for as long as that project has been reviewed by the DIRB. The DIRB Open Action Item Report contains the following information:

- **Project Identification.** Project Identification includes the name of the investment. The Component IT Manager is ultimately responsible for completing all action items. The Exec. Sec. will assist him/her as necessary.
- **Action Items**. Each action item is assigned an action item ID and is accompanied by the date an action item was assigned, any comments the PMO may have on the action item and a short description of the Action Items or tasks that the Component IT Project Manager must complete in order to address DIRB concerns raised at the Review Meeting. These tasks may include management actions, preparation of additional documentation and follow-up meetings.

A sample DIRB Open Action Item Report is shown on the next page.



Open Action Item Report

Action Item ID	*Open Date*	*Description*	*PMO Comments*
Investment Name			
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Investment Name			
I Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x

Date

Page 1 of 1

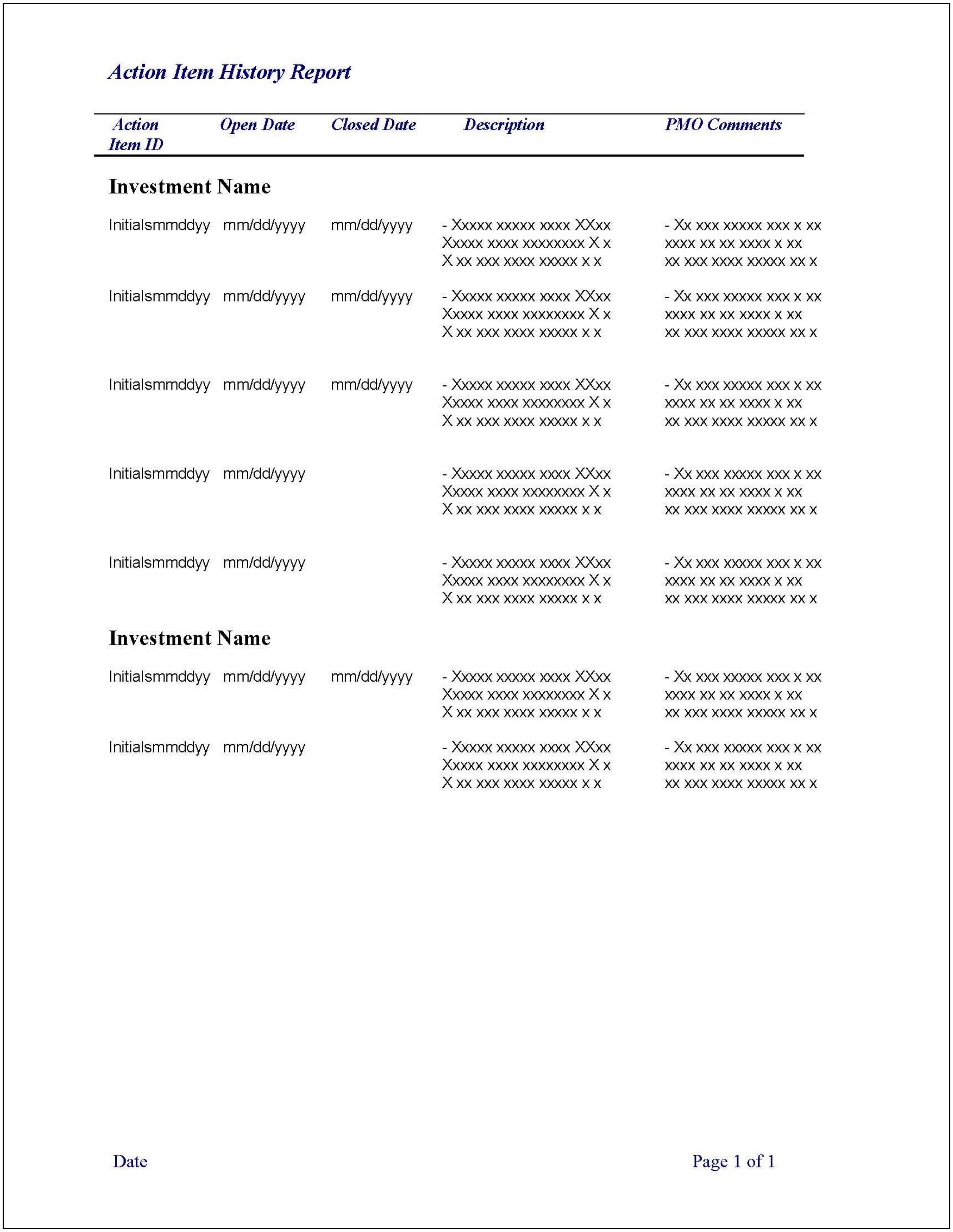
Figure E-1. Sample DIRB Open Action Item Report

E.2 DIRB Action Item History Report

The DIRB Exec. Sec. prepares and maintains the DIRB Action Item History Report to document and monitor the completion of action items assigned to Component IT Project Managers by the DIRB. It contains all action items assigned to a specific project by the DIRB for as long as that project has been reviewed by the DIRB. All action items are included regardless of the status. The DIRB Action Item History Report contains the following information:

- **Project Identification.** Project Identification includes the name of the investment. The Component IT Manager is ultimately responsible for completing all action items. The Exec. Sec. will assist him/her as necessary.
- **Action Items**. Each action item is assigned an action item ID and is accompanied by the date an action item was assigned, the date an action item was closed, any comments the PMO may have on the action item and a short description of the Action Items or tasks that the Component IT Project Manager must complete in order to address DIRB concerns raised at the Review Meeting. These tasks may include management actions, preparation of additional documentation and follow-up meetings.
- **Completion Date**. The Completion Date shows the date the action item was completed. If an action item has not been closed out, this column will be left blank.

A sample DIRB Action Item History Report is shown on the next page.



Action Item History Report

Action Item ID	*Open Date*	*Closed Date*	*Description*	*PMO Comments*
Investment Name				
Initialsmmddyy	mm/dd/yyyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy		- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy		- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Investment Name				
Initialsmmddyy	mm/dd/yyyy	mm/dd/yyyy	- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x
Initialsmmddyy	mm/dd/yyyy		- Xxxxx xxxxx xxxx XXxx Xxxxx xxxx xxxxxxxx X x X xx xxx xxxx xxxxx x x	- Xx xxx xxxxx xxx x xx xxxx xx xx xxxx x xx xx xxx xxxx xxxxx xx x

Date

Page 1 of 1

Figure E-2. DIRB Action Item History Report

E.3 DIRB Project Review Template

Before each DIRB review meeting, the DIRB Executive Secretariat (Exec. Sec.) sends the DIRB Project Review Template to the Component IT Project Manager. The DIRB Review Template is a set of preformatted briefing slides designed to organize the Component IT Project Manager's presentation into three segments:

- **Right Thing.** Right Thing identifies what the project is, how it applies to the Department's mission and strategic goals, the business case, where the project is in its development and presents a lifecycle plan and schedule for the project.
- **Right Way**. Right Way addresses the funding status and budgetary needs of the investment and project progress. It analyzes project status in areas including, but not limited to funding, user involvement, project management and control, cross-government collaboration and IT security.
- **Right Result**. Right Result looks at the project's return on investment (ROI). It looks at business results achieved or expected, cost savings achieved or expected and project risks and planned mitigation strategies.

The Component IT Project Manager fills out the briefing template as appropriate, reviews a draft of the briefing with the DIRB Exec. Sec. and provides the final version of the briefing for distribution to the DIRB members at least one business day before the DIRB Review Meeting.

The latest version of the DIRB Review Template is available for download from the DOJNet intranet on the DOJ OCIO website DIRB webpage.

E.4 DIRB Meeting Summary Template

After each DIRB Review Meeting is completed, the DIRB Exec. Sec. prepares a Meeting Summary report. The Summary captures:

- **The DIRB Vote.** The DIRB Vote will determine the Project Status in the area of Project Issues and Project Management
- **Action Items.** Action Items are a list of actions that the Component IT Manager must complete before the next scheduled DIRB Project Review Meeting
- **Meeting Highlights.** Meeting Highlights capture the issues and themes raised during discussion

The Meeting Summary is reviewed by the Component IT Project Manager for accuracy and approved by the DOJ CIO for release. Once it is approved, the Exec. Sec. distributes the approved summary to all DIRB members and posts the file in the DIRB Summaries directory.

The Meeting Summary template is shown on the following page.

Appendix E

U.S. Department of Justice
Department Investment Review Board

INVESTMENT:	Program Name	
COMPONENT:	Component/Division	
REVIEW DATE:	Month Date, Year	
INCOMING STATUS:	YELLOW/GREEN	
DIRB VOTE:	**Project Issues:**	**RED/YELLOW/GREEN**
	Project Management:	**RED/YELLOW/GREEN**
PMO LEAD:	Name (component)	
DIRB ATTENDEES:	(DAG), (CIO), (Assistant AG for Administration), (Deputy CIO, ESS), (Deputy CIO, PPS), (Controller), (CTO), (Chief Architect), (OCIO)	
ODAG REPRESENTATIVE:	Name (ODAG)	
MEMBERS NOT PRESENT:	Name (component)	
COMPONENT CIO:	Name (component)	
OTHER PMO:	Name (component)	
OTHER DOJ/JMD:	Name (component)	
EXEC SEC:	Name (OCIO)	

The following documents the results of the Department Investment Review Board (DIRB) review.

PROJECT ISSUES:

- Description of the key issues effecting the project progress or outcome.

ACTION ITEMS

The DIRB directs the *Program* PMO to do the following:

- Report to the DIRB by *date* for *action item*.
- X
- Y

Note: The following Discussion Notes sections capture key points and issues raised during the DIRB, not minutes or exact dialogue. The focus is on gathering the most salient discussion points and grouping them by topic.

DISCUSSION NOTES (DIRB + PMO)

Action Item Status:

- X
- Y

Topic:

- X
- Y

DISCUSSION NOTES (DIRB ONLY)

- X
- Y

E.5 Cost/Schedule/Risk Project Status Report

The Project Status Report is a detailed report used by the DOJ OCIO Enterprise Solutions Staff (ESS) to monitor the progress of selected Department-level projects that are required to report progress via DOJ CIO Project Dashboard. The Project Status Report is prepared monthly using information provided by the project manager. The report includes information on the current fiscal year and cumulative earned value data for the project; cost and schedule variance report information; the top five project risks for the project including the risk description, impact, mitigation strategy and mitigation accomplishments; and the key upcoming milestones for the project. The Earned Value report provides a cumulative summary by month of the earned value data for the project over the current fiscal year.

A sample Project Status Report and Earned Value Data report is shown on the following two pages.

Appendix E

(Project Name) Project Review Report

Status through (Month) (Day), (Year)

DOJ Component:
Project Name:
Project Description:
Status Description:

FY 2007 Earned Value Data (through (Month) (Day), (Year))						
BCWS	ACWP	BCWP	SV	CV	CPI	SPI

FY ’07 Projected BCWS:

FY ’07 Budget at Complete:

Cumulative Earned Value Data (through (Month) (Day), (Year))						
BCWS	ACWP	BCWP	SV	CV	CPI	SPI

The monthly earned value data and graph are located in the appendix at the end of this report.

Cost Variance Analysis Report
Cause of the Cost Variance:
Impact to the Project:
Corrective Action:

Schedule Variance Analysis Report
Cause of the Schedule Variance:
Impact to the Project:
Corrective Action:

Top Five Project Risks

Risk Rank: 1	**Status Indicator:**
Risk Description:	
Risk Impact:	
Mitigation Strategy:	
Mitigation Accomplishments:	

Risk Rank: 2	**Status Indicator:**
Risk Description:	
Risk Impact:	
Mitigation Strategy:	
Mitigation Accomplishments:	

Risk Rank: 3	**Status Indicator:**
Risk Description:	
Risk Impact:	
Mitigation Strategy:	

Mitigation Accomplishments:

Risk Rank: 4	**Status Indicator:**
Risk Description:	
Risk Impact:	
Mitigation Strategy:	
Mitigation Accomplishments:	

Risk Rank: 5	**Status Indicator:**
Risk Description:	
Risk Impact:	
Mitigation Strategy:	
Mitigation Accomplishments:	

Next Five Milestones

Milestone Number: 1			
Milestone Description:			
	Baseline	Revised	Actual
Start Date:			
End Date:			

Milestone Number: 2			
Milestone Description:			
	Baseline	Revised	Actual
Start Date:			
End Date:			

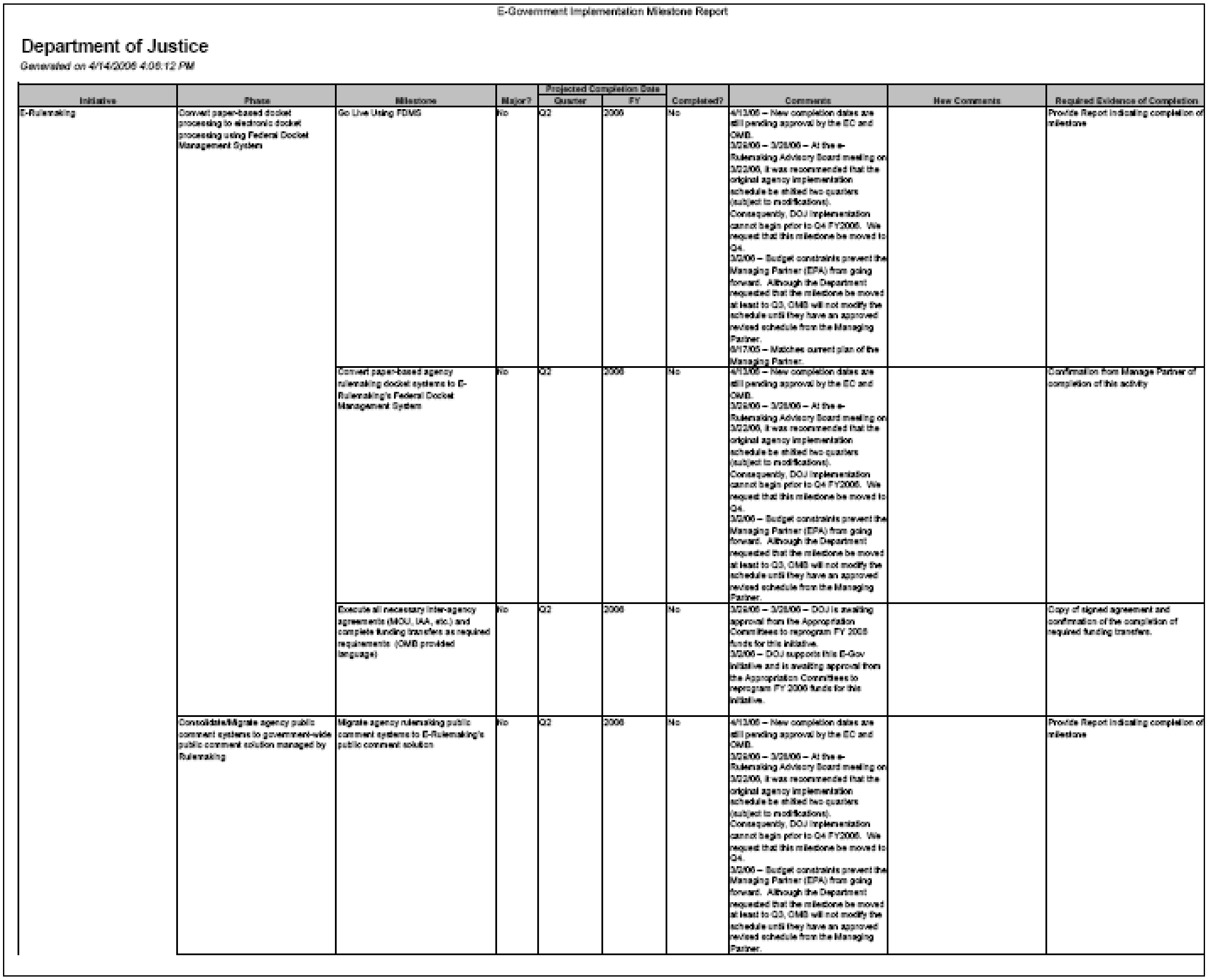
Milestone Number: 3			
Milestone Description:			
	Baseline	Revised	Actual
Start Date:			
End Date:			

Milestone Number: 4			
Milestone Description:			
	Baseline	Revised	Actual
Start Date:			
End Date:			

Milestone Number: 5			
Milestone Description:			
	Baseline	Revised	Actual
Start Date:			
End Date:			

E.6 E-Government Implementation Milestone Report

The E-Government Implementation Milestone Report is a quarterly report submitted to OMB by the E-Government Services Staff. The report provides a status of the completion of all E-Government implementation milestones that are scheduled for completion in a quarter. The report worksheet is provided by OMB twice during the quarter to record the progress in completing the scheduled milestones. The E-Government Services Staff updates the report and returns it to OMB by Day 75 (interim report) and no later than Day 90 (final report) of each quarter. The current report format is shown below.



E-Government Implementation Milestone Report

Department of Justice

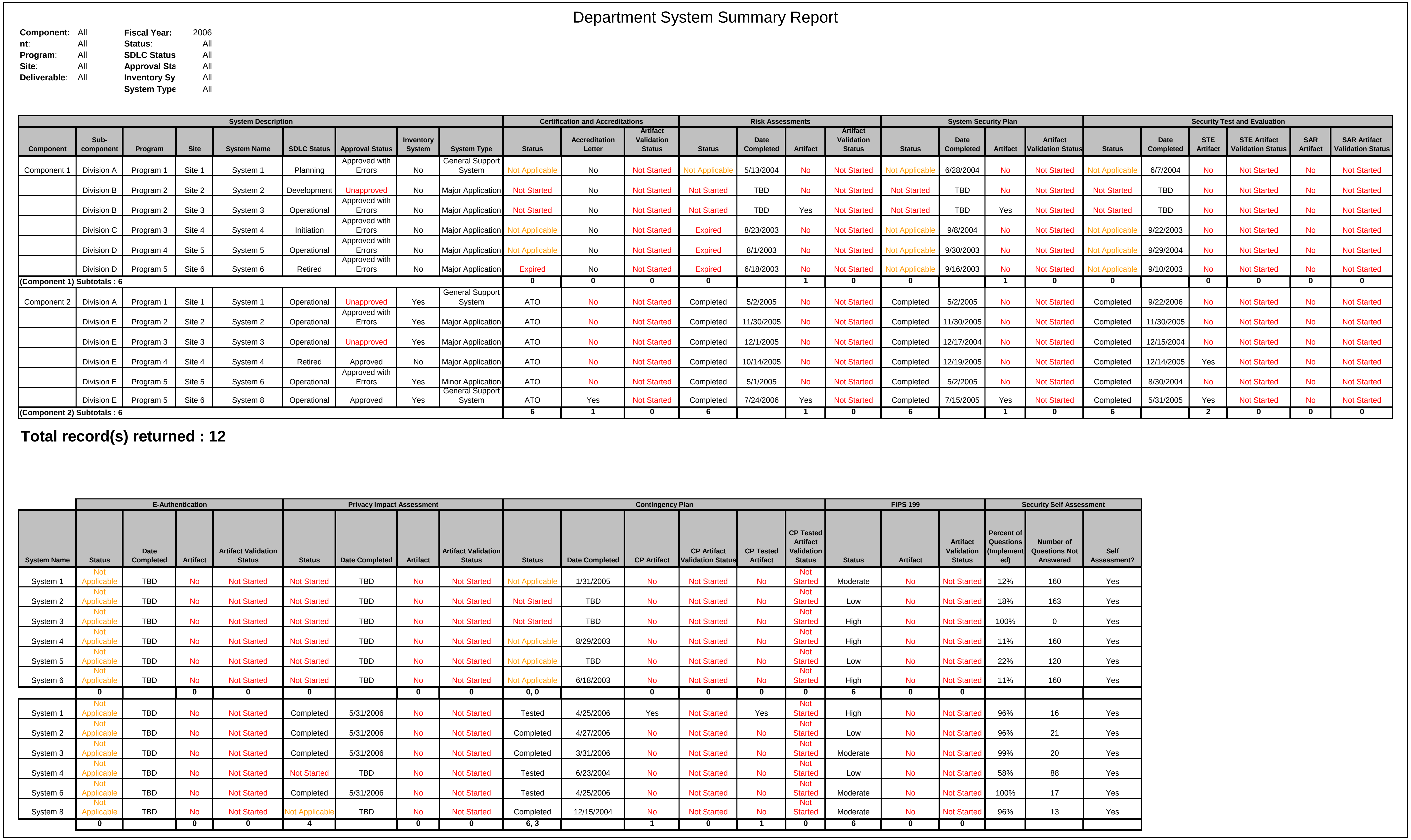
Generated on 4/14/2006 4:08:12 PM

Initiative	Phase	Milestone	Major?	Projected Completion Date		Completed?	Comments	New Comments	Required Evidence of Completion
				Quarter	FY				
E-Rulemaking	Convert paper-based docket processing to electronic docket processing using Federal Docket Management System	Go Live Using FDMS	No	Q2	2006	No	4/13/06 – New completion dates are still pending approval by the EC and OMB. 3/22/06 – 3/28/06 – At the e-Rulemaking Advisory Board meeting on 3/22/06, it was recommended that the original agency implementation schedule be shifted two quarters (subject to modifications). Consequently, DOJ implementation cannot begin prior to Q4 FY2006. We request that this milestone be moved to Q4. 3/2/06 – Budget constraints prevent the Managing Partner (EPA) from going forward. Although the Department requested that the milestone be moved at least to Q3, OMB will not modify the schedule until they have an approved revised schedule from the Managing Partner. 6/17/05 – Matches current plan of the Managing Partner.		Provide Report indicating completion of milestone
		Convert paper-based agency rulemaking docket systems to E-Rulemaking's Federal Docket Management System	No	Q2	2006	No	4/13/06 – New completion dates are still pending approval by the EC and OMB. 3/22/06 – 3/28/06 – At the e-Rulemaking Advisory Board meeting on 3/22/06, it was recommended that the original agency implementation schedule be shifted two quarters (subject to modifications). Consequently, DOJ implementation cannot begin prior to Q4 FY2006. We request that this milestone be moved to Q4. 3/2/06 – Budget constraints prevent the Managing Partner (EPA) from going forward. Although the Department requested that the milestone be moved at least to Q3, OMB will not modify the schedule until they have an approved revised schedule from the Managing Partner.		Confirmation from Manage Partner of completion of this activity
		Execute all necessary inter-agency agreements (MOU, IAA, etc.) and complete funding transfers as required requirements (OMB provided language)	No	Q2	2006	No	3/28/06 – 3/28/06 – DOJ is awaiting approval from the Appropriation Committees to reprogram FY 2006 funds for this initiative. 3/2/06 – DOJ supports this E-Gov initiative and is awaiting approval from the Appropriation Committees to reprogram FY 2006 funds for this initiative.		Copy of signed agreement and confirmation of the completion of required funding transfers.
	Consolidate/Migrate agency public comment systems to government-wide public comment solution managed by Rulemaking	Migrate agency rulemaking public comment systems to E-Rulemaking's public comment solution	No	Q2	2006	No	4/13/06 – New completion dates are still pending approval by the EC and OMB. 3/22/06 – 3/28/06 – At the e-Rulemaking Advisory Board meeting on 3/22/06, it was recommended that the original agency implementation schedule be shifted two quarters (subject to modifications). Consequently, DOJ implementation cannot begin prior to Q4 FY2006. We request that this milestone be moved to Q4. 3/2/06 – Budget constraints prevent the Managing Partner (EPA) from going forward. Although the Department requested that the milestone be moved at least to Q3, OMB will not modify the schedule until they have an approved revised schedule from the Managing Partner.		Provide Report indicating completion of milestone

Figure E-3. E-Government Implementation Milestone Report.

E.7 IT Security Staff Department System Summary Report

The IT Security Staff Department System Summary Report provides a complete profile of the security compliance status for all IT systems registered in the IT Security Staff's FISMA/ Trusted Agent tracking system. The information collected for the report serves as the basis for the ratings that appear on the IT Security Scorecard in the FISMA/Trusted Agent system. The IT Security Scorecard provides a visual indicator (Green, Yellow, or Red) of IT security compliance status for each IT system or application, as well as a summary status for each Component. The System Summary Report example on the following page has been condensed so the reader can see the information monitored by the IT Security Staff and the system information contained in the summary report.



Department System Summary Report

Component:	All	**Fiscal Year:**	2006
nt:	All	**Status**:	All
Program:	All	**SDLC Status**	All
Site:	All	**Approval Sta**	All
Deliverable:	All	**Inventory Sy**	All
		System Type	All

System Description									Certification and Accreditations			Risk Assessments				System Security Plan				Security Test and Evaluation					
Component	**Sub-component**	**Program**	**Site**	**System Name**	**SDLC Status**	**Approval Status**	**Inventory System**	**System Type**	**Status**	**Accreditation Letter**	**Artifact Validation Status**	**Status**	**Date Completed**	**Artifact**	**Artifact Validation Status**	**Status**	**Date Completed**	**Artifact**	**Artifact Validation Status**	**Status**	**Date Completed**	**STE Artifact**	**STE Artifact Validation Status**	**SAR Artifact**	**SAR Artifact Validation Status**
Component 1	Division A	Program 1	Site 1	System 1	Planning	Approved with Errors	No	General Support System	Not Applicable	No	Not Started	Not Applicable	5/13/2004	No	Not Started	Not Applicable	6/28/2004	No	Not Started	Not Applicable	6/7/2004	No	Not Started	No	Not Started
	Division B	Program 2	Site 2	System 2	Development	Unapproved	No	Major Application	Not Started	No	Not Started	Not Started	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Started	TBD	No	Not Started	No	Not Started
	Division B	Program 2	Site 3	System 3	Operational	Approved with Errors	No	Major Application	Not Started	No	Not Started	Not Started	TBD	Yes	Not Started	Not Started	TBD	Yes	Not Started	Not Started	TBD	No	Not Started	No	Not Started
	Division C	Program 3	Site 4	System 4	Initiation	Approved with Errors	No	Major Application	Not Applicable	No	Not Started	Expired	8/23/2003	No	Not Started	Not Applicable	9/8/2004	No	Not Started	Not Applicable	9/22/2003	No	Not Started	No	Not Started
	Division D	Program 4	Site 5	System 5	Operational	Approved with Errors	No	Major Application	Not Applicable	No	Not Started	Expired	8/1/2003	No	Not Started	Not Applicable	9/30/2003	No	Not Started	Not Applicable	9/29/2004	No	Not Started	No	Not Started
	Division D	Program 5	Site 6	System 6	Retired	Approved with Errors	No	Major Application	Expired	No	Not Started	Expired	6/18/2003	No	Not Started	Not Applicable	9/16/2003	No	Not Started	Not Applicable	9/10/2003	No	Not Started	No	Not Started
(Component 1) Subtotals : 6									**0**	**0**	**0**	**0**		**1**	**0**	**0**		**1**	**0**	**0**		**0**	**0**	**0**	**0**
Component 2	Division A	Program 1	Site 1	System 1	Operational	Unapproved	Yes	General Support System	ATO	No	Not Started	Completed	5/2/2005	No	Not Started	Completed	5/2/2005	No	Not Started	Completed	9/22/2006	No	Not Started	No	Not Started
	Division E	Program 2	Site 2	System 2	Operational	Approved with Errors	Yes	Major Application	ATO	No	Not Started	Completed	11/30/2005	No	Not Started	Completed	11/30/2005	No	Not Started	Completed	11/30/2005	No	Not Started	No	Not Started
	Division E	Program 3	Site 3	System 3	Operational	Unapproved	Yes	Major Application	ATO	No	Not Started	Completed	12/1/2005	No	Not Started	Completed	12/17/2004	No	Not Started	Completed	12/15/2004	No	Not Started	No	Not Started
	Division E	Program 4	Site 4	System 4	Retired	Approved	No	Major Application	ATO	No	Not Started	Completed	10/14/2005	No	Not Started	Completed	12/19/2005	No	Not Started	Completed	12/14/2005	Yes	Not Started	No	Not Started
	Division E	Program 5	Site 5	System 6	Operational	Approved with Errors	Yes	Minor Application	ATO	No	Not Started	Completed	5/1/2005	No	Not Started	Completed	5/2/2005	No	Not Started	Completed	8/30/2004	No	Not Started	No	Not Started
	Division E	Program 5	Site 6	System 8	Operational	Approved	Yes	General Support System	ATO	Yes	Not Started	Completed	7/24/2006	Yes	Not Started	Completed	7/15/2005	Yes	Not Started	Completed	5/31/2005	Yes	Not Started	No	Not Started
(Component 2) Subtotals : 6									**6**	**1**	**0**	**6**		**1**	**0**	**6**		**1**	**0**	**6**		**2**	**0**	**0**	**0**

Total record(s) returned : 12

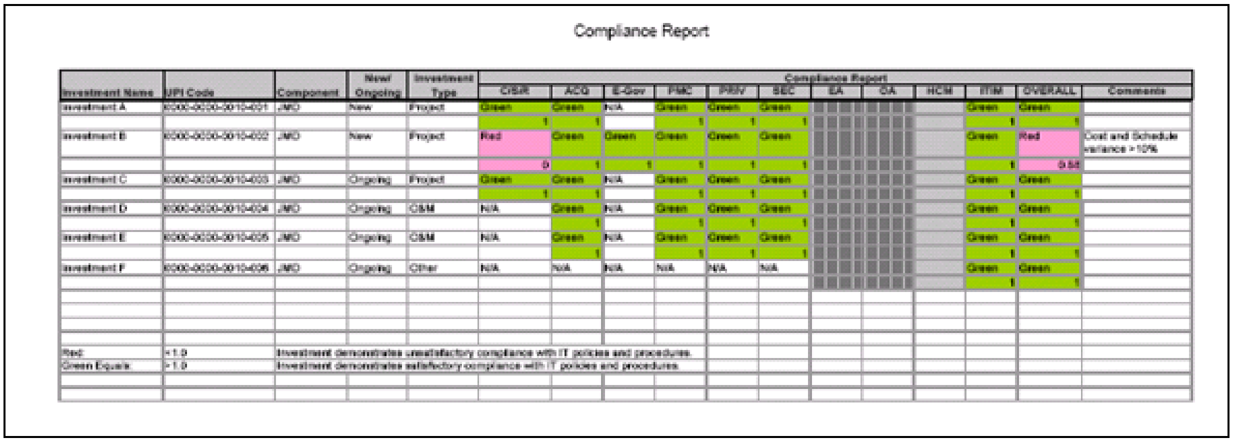
	E-Authentication				Privacy Impact Assessment				Contingency Plan						FIPS 199			Security Self Assessment		
System Name	**Status**	**Date Completed**	**Artifact**	**Artifact Validation Status**	**Status**	**Date Completed**	**Artifact**	**Artifact Validation Status**	**Status**	**Date Completed**	**CP Artifact**	**CP Artifact Validation Status**	**CP Tested Artifact**	**CP Tested Artifact Validation Status**	**Status**	**Artifact**	**Artifact Validation Status**	**Percent of Questions (Implemented)**	**Number of Questions Not Answered**	**Self Assessment?**
System 1	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Applicable	1/31/2005	No	Not Started	No	Not Started	Moderate	No	Not Started	12%	160	Yes
System 2	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Started	TBD	No	Not Started	No	Not Started	Low	No	Not Started	18%	163	Yes
System 3	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Started	TBD	No	Not Started	No	Not Started	High	No	Not Started	100%	0	Yes
System 4	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Applicable	8/29/2003	No	Not Started	No	Not Started	High	No	Not Started	11%	160	Yes
System 5	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Applicable	TBD	No	Not Started	No	Not Started	Low	No	Not Started	22%	120	Yes
System 6	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Not Applicable	6/18/2003	No	Not Started	No	Not Started	High	No	Not Started	11%	160	Yes
	0		**0**	**0**	**0**		**0**	**0**	**0, 0**		**0**	**0**	**0**	**0**	**6**	**0**	**0**			
System 1	Not Applicable	TBD	No	Not Started	Completed	5/31/2006	No	Not Started	Tested	4/25/2006	Yes	Not Started	Yes	Not Started	High	No	Not Started	96%	16	Yes
System 2	Not Applicable	TBD	No	Not Started	Completed	5/31/2006	No	Not Started	Completed	4/27/2006	No	Not Started	No	Not Started	Low	No	Not Started	96%	21	Yes
System 3	Not Applicable	TBD	No	Not Started	Completed	5/31/2006	No	Not Started	Completed	3/31/2006	No	Not Started	No	Not Started	Moderate	No	Not Started	99%	20	Yes
System 4	Not Applicable	TBD	No	Not Started	Not Started	TBD	No	Not Started	Tested	6/23/2004	No	Not Started	No	Not Started	Low	No	Not Started	58%	88	Yes
System 6	Not Applicable	TBD	No	Not Started	Completed	5/31/2006	No	Not Started	Tested	4/25/2006	No	Not Started	No	Not Started	Moderate	No	Not Started	100%	17	Yes
System 8	Not Applicable	TBD	No	Not Started	Not Applicable	TBD	No	Not Started	Completed	12/15/2004	No	Not Started	No	Not Started	Moderate	No	Not Started	96%	13	Yes
	0		**0**	**0**	**4**		**0**	**0**	**6, 3**		**1**	**0**	**1**	**0**	**6**	**0**	**0**			

Figure E-4. Department System Summary Report

Blank Page

E.8 Compliance Report

The Compliance Report summarizes the compliance review information for active investments into a single report that is used during investment planning and budget planning to inform decision makers about the compliance condition of ongoing investments. The OCIO Policy and Planning Staff (PPS) accumulates the individual compliance ratings for each of the compliance areas from the OCIO Compliance Managers responsible for each review. PPS then assigns a summary compliance rating that reflects the overall compliance condition for each investment. This information is provided to the DOJ CIO as part of the consolidated Exhibit 51/53 for consideration during review of the Spring IT Budget. A sample of the Compliance Report is shown below.



Compliance Report

			New/	Investment	Compliance Report											
Investment Name	UPI Code	Component	Ongoing	Type	C/S/R	ACQ	E-Gov	PMC	PRIV	SEC	EA	OA	HCM	ITIM	OVERALL	Comments
Investment A	0000-0000-0010-001	JMD	New	Project	Green	Green	N/A	Green	Green	Green				Green	Green	
					1	1		1	1	1				1	1	
Investment B	0000-0000-0010-002	JMD	New	Project	Red	Green	Green	Green	Green	Green				Green	Red	Cost and Schedule variance > 10%
					0	1	1	1	1	1				1	0.58	
Investment C	0000-0000-0010-003	JMD	Ongoing	Project	Green	Green	N/A	Green	Green	Green				Green	Green	
					1	1		1	1	1				1	1	
Investment D	0000-0000-0010-004	JMD	Ongoing	O&M	N/A	Green	N/A	Green	Green	Green				Green	Green	
						1		1	1	1				1	1	
Investment E	0000-0000-0010-005	JMD	Ongoing	O&M	N/A	Green	N/A	Green	Green	Green				Green	Green	
						1		1	1	1				1	1	
Investment F	0000-0000-0010-006	JMD	Ongoing	Other	N/A	N/A	N/A	N/A	N/A	N/A				Green	Green	
														1	1	
Red:	<1.0	Investment demonstrates unsatisfactory compliance with IT policies and procedures.														
Green Equals:	>1.0	Investment demonstrates satisfactory compliance with IT policies and procedures.														

Figure E-5. Compliance Report

Blank Page